УДК 621.391.25
DOI: 10.15587/1729-4061.2018.139755

Підвищення продуктивності генерації випадкових послідовностей для систем захисту інформації

С. О. Іванченко, С. П. Євсеєв, В. М. Безштанько, В. М. Бондаренко, О. В. Гавриленко, Н. Ф. Казакова, Р. В. Корольов, С. Ю. Мазор, В. П. Романенко, О. О. Фразе-Фразенко

Обґрунтовано шляхи підвищення продуктивності генерації випадкових послідовностей, що утворені від фізичних джерел, для систем захисту інформації. Це потрібно тому, що на сьогоднішній день відбувається бурхливе зростання технологічних можливостей та швидкісних показників реалізації різноманітних інформаційних сервісів та додатків, що потребує спільнота. Одним з головних питань безпечного використання цих сервісів є гарантування інформаційної безпеки, яка вимагає використання ефективних швидкодіючих систем захисту інформації та високопродуктивної генерації послідовностей випадкових даних. При проведенні досліджень з метою підвищення продуктивності здійснено аналіз особливості перетворення реальних шумових процесів з врахуванням їх нестаціонарності та відхилень від розподілу ймовірностей. Запропоновано шляхи вдосконалення методів аналого-цифрового перетворення з оптимізацією шкали квантування динамічного діапазону та кроку дискретизації шумового процесу в часі. З метою вирівнювання статистичних характеристик розглянуто можливість використання методів обробки, які підвищують її статистичну якість з економією швидкісних втрат. Це метод вибірки рівноймовірних комбінацій (von Neuman – Elias – Рябко – Мачикиної) та метод кодової оброки (Santha – Vazirani), які завдяки розширення коду забезпечують певну ефективність та полягають в перетворенні послідовності: в першому з використанням рівноймовірніх комбінацій з відкиданням непотрібних даних, в другому без їх відкидання з можливістю лінійного перетворення. З метою оптимізації параметрів перетворення на обох етапах генерації та адаптації цих параметрів до особливостей і змінності характеристик перетворюваних випадкових процесів запропоновано використання зворотних зв'язків виходів перетворювачів з попередніми елементами перетворення. Коригування вказаних параметрів має здійснюватись під час генерації за результатами статистичного аналізу виходів етапів перетворення. Отримані результати є досить важливими, оскілки їх реалізація в сучасних системах захисту інформації дозволить гарантоване забезпечення інформаційної безпеки та безпечне використання додатків сучасного інформаційного сервісу та впровадження нових додатків

Ключові слова: випадкові дані, шумові процеси, захист інформації, перетворення, обробка, статистичне вирівнювання

1. Вступ

На сьогоднішній день з розвитком науки і техніки відбувається бурхливе зростання технічних та технологічних можливостей реалізації різноманітних інформаційних сервісів та додатків, що потребує спільнота. Сучасні інформаційні технології забезпечують виконання завдань різної складності з обробкою та передаванням великих масивів даних, різноманітними обчисленнями та прийняттям рішень. Відповідно, вони вимагають задіяння великих машинних ресурсів, для яких одним із основних показників є швидкість роботи інформаційних систем, що використовуються. Зазначена швидкість забезпечує швидкодію та складність реалізованих технологій.

Одним з центральних питань безпечного використання сучасних інформаційних сервісів та додатків є гарантування інформаційної безпеки, яка вимагає використання ефективних систем захисту інформації. Потреби зростання швидкодії інформаційних технологій приводять до відповідних потреб в швидкодії систем захисту інформації. В свою чергу, ці системи вимагають високої продуктивності генераторного обладнання та послідовностей випадкових даних.

Окремим питанням, що також сприяє необхідності підвищення продуктивності генераторів, є зростання потенційних можливостей реалізації загроз та ефективних методів статистичного аналізу. Адже статистичний аналіз випадкових послідовностей дозволяє виявлення слабких місць, що зменшують їх практичну невизначеність.

Існує багато технологій та додатків [1–10], які потребують використання послідовностей випадкових даних. Це імітаційне моделювання, яке надає можливість дослідження реальних об’єктів (процесів), замінивши моделями [1]. Це криптографічні додатки, які забезпечують конфіденційність інформації завдяки перетворенням з використанням випадкового ключа [2, 3]. Це рандомізація даних для убезпечення інформації від витоку технічними каналами [4–6]. Це цифрова генерація завад для маскування небезпечних сигналів в каналах витоку [7–10], генерація паролів, захисних кодів, тощо.

Таким чином, для безпечного використання сучасних інформаційних сервісів та додатків та забезпечення ефективного захисту інформації послідовності випадкових даних мають вироблятись з заданою якістю та заданою швидкістю – продуктивністю, вимога щодо якої постійно зростає.

2. Аналіз літературних даних та сутність проблеми

На даний час всі методи та засоби генерації послідовностей випадкових даних можна розділити в два покоління. Одне з них – це діюче покоління. Воно включає традиційні методи, що вже мають реалізації у виді технічних засобів. Як правило, ці методи базуються на перетворенні деяких природних процесів – фізичних джерел, які мають ознаки випадковості в тій чи іншій мірі. Зазначені методи досить повно описані в працях [11, 12].

Суттєвим недоліком цих методів та засобів є низька швидкість генерації, або наявність в послідовностях статистичних дефектів. Усунення цих дефектів вимагає вирівнювання статистичних характеристик, які знову ж таки здійснюються за рахунок зниження швидкості. Методи цього покоління є ни-

зькопродуктивними та не спроможні достатньо забезпечити потреби сучасних систем захисту.

Наступним поколінням є новітні методи генерації послідовностей випадкових даних, головною відмінністю яких від діючих є те, що вони базуються на квантово-механічній теорії. Вони використовують не перетворення фізичних випадкових процесів у послідовність, а сама послідовність вже є випадковим процесом, сформованим від спінових станів елементарних частинок (електронів, протонів, нейтронів). Відповідно теоремі Джона Белла (1964р.) генерація зазначеним способом може на великих швидкостях забезпечити повну невизначеність послідовності. Тому вивченню цього питання присвячено багато наукових праць.

Так, в роботі [13] розглянуті можливості отримання незалежних випадкових двійкових даних на основі квантово-механічного представлення природних процесів (явищ), які задовольняють критерій невиконання нерівності Белла. В роботі [14] в противагу класичній фізиці, яка виключає існування випадковості в повному розумінні цього слова, запропонований тест Белла, який за принципом квантової теорії дозволяє отримання послідовності випадкових біт. В роботі [15] обґрунтуванні моделі отримання випадковості з не взаємодіючих та ненадійних квантових пристроїв. Запропонований спосіб побудови екстрактору випадковості є захищеним від сучасних квантових атак.

В роботі [16] показано можливість підсилення слабкої випадковості з використанням квантових ресурсів. Наведений протокол підсилення випадковості, що включає експерименти Белла з достатнім невиконанням його нерівності. Робота [17] присвячена забезпеченню випадковістю квантової криптографії, доведена безпека нового протоколу та обґрунтована захищеність відносно квантових атак. В роботі [18] продемонстровано апаратна реалізація генератора швидких випадкових чисел с фотонною інтегральною схемою та електронною платою програмованої вентильної матриці.

Попри все ці квантово-механічні методи генерації ще не зазнали достатньої повноти в реалізаціях. Незважаючи на існування певних зразків квантової техніки, вони поки що залишаються в статусі перспективних. Адже ця техніка використовує принципово новітні фізичні ефекти, де в якості носіїв даних використовуватиметься не електричний струм, а кванти енергії – спіни елементарних частинок. Вона на даний час носить більше експериментальний характер ніж користувальний та вимагає відповідного розвитку.

В окремий клас методів стосовно отримання послідовностей випадкових даних можна виділити методи псевдовипадкової генерації, що ґрунтуються на алгоритмічній складності [2, 3]. Суттєвою перевагою останніх є досягнення потрібної швидкості генерації, яка визначається тактовою частотою засобу, що реалізує алгоритм. Цим методам також присвячено ряд відповідних праць. Зокрема, в роботі [19] розглянуті методи побудови цих генераторів, їх теоретичні та емпіричні властивості з потрібним порівнянням. Робота [20] присвячена застосуванню генераторів випадкових послідовностей для формування криптографічних ключів та, в зв’язку з жорсткістю вимог до них, можливості заміни цих генераторів псевдовипадковими генераторами. В роботі [21] розглянуті

можливості реалізації псевдовипадкових даних на базі програмованих логічних інтегральних схем, де були показані досить високі швидкості генерації.

Однак, незважаючи на близькість статистичних характеристик псевдовипадкових даних до випадкових та можливості забезпечення потрібних швидкостей генерації, псевдовипадковість із-за алгоритмічного походження дозволяє вираховування та відгадування даних послідовності. Це є небажаним для систем захисту інформації та обмежує використання в них методів псевдовипадкової генерації.

Таким чином, проведений аналіз показав, що методи генерації послідовностей на основі аналого-цифрового перетворення шумових процесів залишаються актуальними та затребуваними. Послідовності випадкових даних для систем захисту потрібні зараз і сьогодні. А тому вони вимагають вдосконалення та ефективного застосування на практиці. Підтвердженням цьому є дослідження останніх років, що опубліковані в наступних працях. В роботі [22] проведено експериментальний аналіз випадковості при генерації випадкових послідовностей на основі аналого-цифрового перетворення. Робота [23] присвячена отриманню випадкових послідовностей на основі аналого-цифрового перетворення виходу напівпровідникового лазера з зовнішнім резонатором. В роботі [24] здійснено опис моделі джерела випадкових двійкових даних від фізичних джерел. Робота [25] присвячена використанню властивостей напівпровідникових лазерів, що працюють в хаотичному режимі.

Однак, підвищення продуктивності в зазначених роботах здійснюється не за рахунок раціонального перетворення шумового процесу, а шляхом використання джерел з розширенням спектру до оптичного діапазону частот. Так, це є досить ефективним підходом щодо підвищення продуктивності, але мають місце й інші шляхи, які також нададуть можливість підвищення продуктивності як при використанні класичних методів аналого-цифрового перетворення шумових процесів з невисокою частотою Найквіста [11, 12, 26], так і з використанням лазерних пристроїв, описаних в роботах [23–25]. Адже теоретично всі неперервні випадкові процеси мають нескінченну ентропію на відлік. Хоча реальні фізичні джерела цих процесів є далеко не ідеальними, все теки від них можна отримати високу продуктивність генерації. Відповідно, підвищення продуктивності генерації вимагає обґрунтування та застосування ефективних методів перетворення.

На даний час, як вже було зазначено, методи генерації випадкових послідовностей від фізичних джерел не завжди відповідають потребам з якісно-швидкісних показників. Як правило, забезпечення потрібної якості здійснюється на низьких швидкостях генерації. Підвищення ж швидкості приводить до зниження якості та появи статистичних дефектів послідовності. Причинами зазначеного є:

– невідповідність параметрів аналого-цифрового перетворення та щільності розподілу ймовірностей перетворюваного випадкового процесу;

– нестаціонарністю використаного для аналого-цифрового перетворення випадкового процесу.

Усунення статистичних недоліків може бути здійсненим шляхом викорис-

тання методів вирівнювання статистичних характеристик, що підвищують ентропію джерела. Ефективними із них є

– метод von Neuman-Elias-Рябко-Мачикиної (вибірки рівноймовірних комбінацій) [27–29];

– метод Santha – Vazirani (кодової оброки лінійним кодом) [30, 31].

Зазначені методи дозволяють досягти високих показників випадковості даних. Однак це здійснюють за рахунок зменшення швидкості генерації, що є суттєвим недоліком цих методів. Підвищення швидкості можливе шляхом укрупнення алфавіту, що вимагає відповідної оптимізації параметрів вирівнюванням та узгодження з етапом аналого-цифрового перетворення.

Таким чином, актуальною науково-технічною проблемою є забезпечення продуктивності існуючих методів та засобів генерації випадкових послідовностей від фізичних джерел, для забезпечення потреб сучасних систем захисту інформації.

При цьому невирішеними є такі завдання:

1. Неоптимізовані чинники та їх параметри, що впливають на підвищення продуктивності аналого-цифрового перетворення шумових процесів в послідовності випадкових даних.

2. Неузгоджена ефективність та не оптимізовані параметри вирівнювання статистичних характеристик випадкових послідовностей з методами аналого-цифрового перетворення.

3. Необґрунтовані завдання та способи адаптації параметрів щодо нестаціонарності перетворюваних процесів на обох етапах генерації: аналого-цифрового перетворення та вирівнювання статистичних характеристик.

3. Мета та задачі дослідження

Метою дослідження є підвищення продуктивності методів генерації випадкових послідовностей на основі оптимізації аналого-цифрового перетворення шумових процесів для забезпечення сучасних систем захисту інформації.

Для досягнення поставленої мети в роботі розглянуті завдання:

– оптимізувати параметри аналого-цифрового перетворення шумових процесів, що впливають на підвищення продуктивності генерації послідовностей випадкових даних;

– обґрунтувати вибір методу, що забезпечують належне вирівнювання статистичних характеристик випадкових послідовностей для систем захисту інформації;

– обґрунтувати способи адаптації параметрів на обох етапах перетворення щодо нестаціонарності перетворюваних процесів та змінності інших факторів, що впливають на продуктивність генерації.

4. Дослідження чинників та шляхів підвищення продуктивності генерації випадкових послідовностей

Для досліджень шляхів підвищення продуктивності генерації випадкових послідовностей від фізичних джерел процес перетворення шумових процесів зручно представити у виді двох етапів перетворення (рис. 1):

1) етап первинного перетворення шумового процесу $u(t)$ у послідовність даних X;

2) етап вторинного перетворення X у послідовність Y з метою усунення статистичних дефектів та вирівнювання статистичних характеристик.

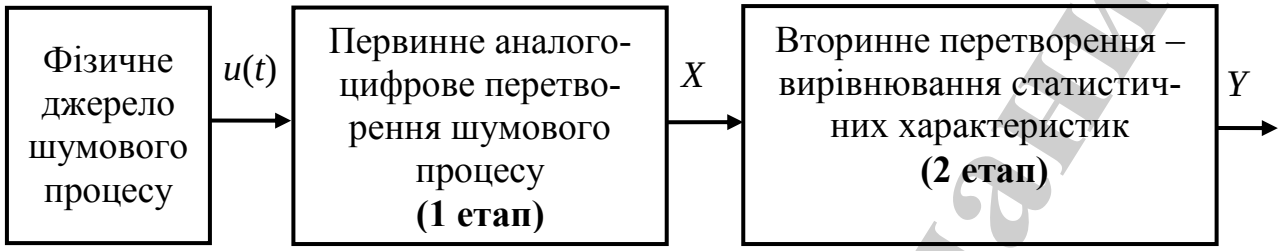

Рис. 1. Схема двох етапної генерації випадкових послідовностей від фізичного джерела з аналого-цифровим перетворенням та вирівнюванням статистичних характеристик

4. 1. Етап первинного перетворення шумового процесу. Обґрунтування чинників та їх параметрів

Нехай має місце фізичне джерело, що формує шумовий процес $u(t)$. Випадковий сигнал $u(t)$ при перетворенні дискретизується в часі з кроком Δt та квантується в динамічному діапазоні з кроком Δu (рис. 2).

Кожне випадкове значення $u=u(t_j)$ у відліках часу з індексами $j=1, 2, 3,\ldots$ округлюється до найближчого квантованого значення u_i, кратного Δu, $i= -N, \ldots, -1, 0, 1,\ldots, N$ (N – натуральне число, що визначає нижню та верхню межі номерів квантилів) так, що $u_i=u(t_j)$. Кожному u_i ставиться у відповідність двійкова комбінація $X_k^n=(x_1, x_2, x_3, \ldots, x_n)$, довжини n, $k=1, 2, 3, \ldots 2^n$. Довжина n обирається з міркування $n \geq \log_2(2N)$ [32].

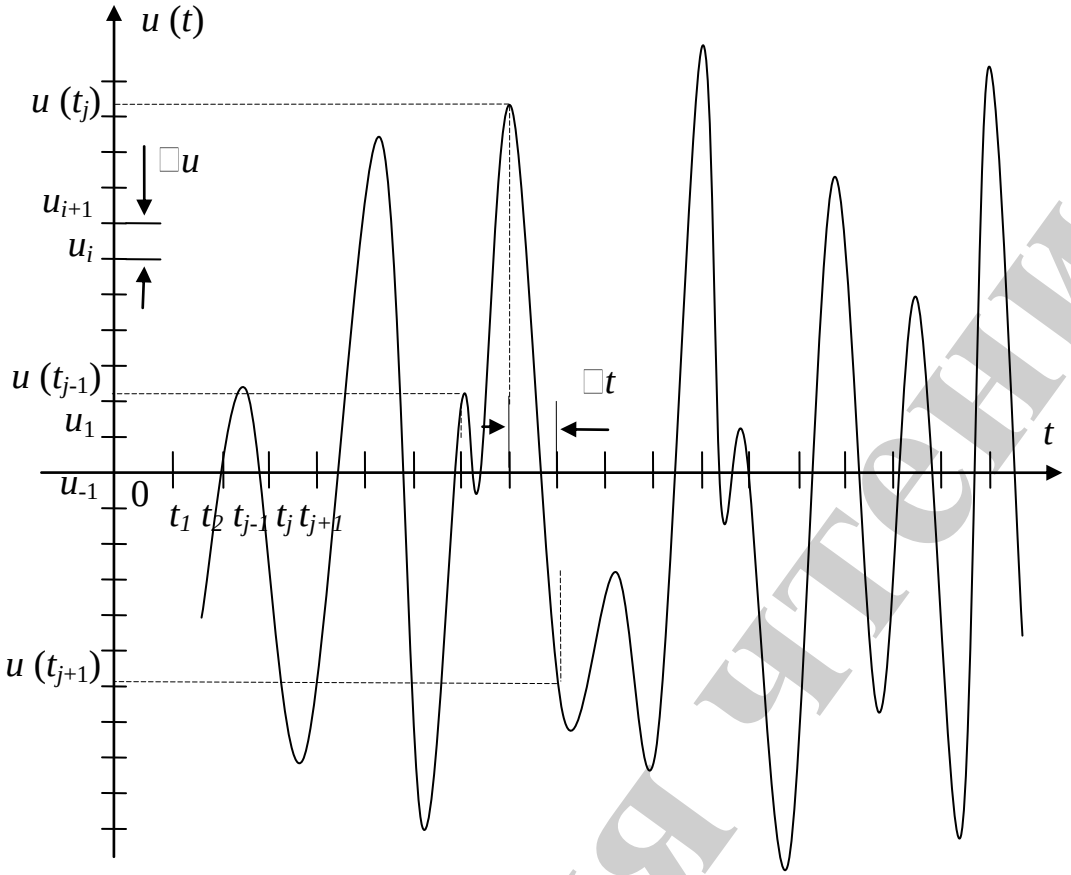

Рис. 2. Сутність перетворення шумового процесу для формування випадкової послідовності

Найпростішим прикладом такого перетворення є метод визначення випадкового знаку за оцінкою рівня шумового процесу у фіксовані моменти часу відносно обраного порога – нуля квантування [11]. Якщо миттєва напруга шуму менше нуля ($u=u_{-1}<0$), то на виході формується логічний нуль ($x=0$), якщо більше ($u=u_1>0$), то одиниця ($x=1$). При цьому за один такт дискретизації виробляється один знак ($n=1$). Цей метод є результатом розробок минулого сторіччя, який відповідає рівню розвитку техніки тих часів, та дозволяє невисоку продуктивність генерації – добуток невизначеності випадкової послідовності та швидкості її формування. Швидкість такої генерації є обмеженою та залежить від частоти Найквіста перетворюваного процесу [26]. При збільшення швидкості у генерованій послідовності даних з'являлись різного характеру статистичні дефекти, що вимагали усунення (статистичного вирівнювання), а ті, в свою чергу, приводили до зниження швидкості. При цьому ефект генерації досягався за рахунок економії у швидкості на етапі вирівнювання.

Іншим, сучасним прикладом перетворення шумових процесів у випадкові послідовності, є відоме аналого-цифрове перетворення. Відрізняється від розглянутого прикладу розширенням у способі перетворення шкали квантування та інтервалу дискретизації. Для тих же випадкових процесів це дозволяє генерацію послідовностей даних на більш високих швидкостях та, відповідно з більш високою продуктивністю. Як зазвичай, для цього використовують уніфіковані

засоби аналого-цифрового перетворення, що мають переважно лінійну шкалу квантування або пропорційну деяким математичним функціям, наприклад, експоненційну чи логарифмічну шкалу. Якщо шумовий процес стаціонарний, то відносно нескладно підібрати шкалу квантування, яка б забезпечувала потрібну статистику вироблених даних.

Реальні шумові процеси є далеко не стаціонарними. Лінійна та інші фіксовані шкали квантування не достатньо адаптовані щодо щільності розподілу. Це є причиною наявності статистичних дефектів в отриманих послідовностях. Зазначені дефекти створюють необхідність застосування до цих послідовностей ефективних методів статистичного вирівнювання.

Таким чином, основними чинниками, що впливають на продуктивність аналого-цифрового перетворення шумових процесів, які визначаються сучасними технічними можливостями реалізації, наприклад, спектрального аналізу, є наступні:

1. Шкала квантування динамічного діапазону випадкового процесу Δu_i, $i = -N, \ldots, -1, 0, 1, \ldots, N$, та кількість рівнів квантування $2N$.

2. Інтервал дискретизації випадкового процесу в часі Δt, що залежить від частотного спектру перетворюваного випадкового процесу.

3. Нестаціонарність та змінність статистичних властивостей перетворюваних процесів.

Як відомо з теорії інформації [33], всі випадкові неперервні процеси, що розраховані на один відлік, мають нескінченно велику ентропію:

$$H(U) = \lim_{\Delta u \to 0} \sum_i \omega(u_i)\Delta u \log_2 \frac{1}{\omega(u_i)\Delta u} =$$

$$= \int_{-\infty}^{\infty} \omega(u) \log_2 \frac{1}{\omega(u)} du + \lim_{\Delta u \to 0} \log_2 \frac{1}{\Delta u} \sum_i \omega(u_i)\Delta u = \qquad (1)$$

$$= h(u) + \lim_{\Delta u \to 0} \log_2 \frac{1}{\Delta u} = \infty,$$

де $h(u)$ – диференційна ентропія.

Хоча, реальні шумові процеси є далеко не ідеальними та ентропія не є нескінченною, все таки ці процеси можуть надати можливість отримання досить високої ентропії, яка залежатиме не тільки від статистичних властивостей випадкового процесу, а й від обраної шкали ненульових Δu.

Для забезпечення високих показників продуктивності завдання генерації послідовностей випадкових даних вимагає оптимізації аналого-цифрового перетворення випадкових процесів.

Критерієм оптимізації цього перетворення є максимум продуктивності генерації:

$$H'(X,Y) = \max[V_{\text{ген.}} H(X,Y)], \qquad (2)$$

де $V_{\text{ген.}}$ – швидкість генерації джерела:

$$V_{\text{ген.}} = \frac{\log_2(2N)}{\Delta t}. \qquad (3)$$

Критерій (2) на обох етапах перетворення може бути забезпеченим виконанням максимуму швидкості за фіксованої якості генерації або максимуму якості за фіксованої швидкості генерації.

Отже, підвищення продуктивності генерування послідовностей випадкових даних на першому етапі зводиться до отримання наступних вирішень:

1. Обґрунтування оптимальної шкали квантування динамічного діапазону щодо статистичних властивостей перетворюваного випадкового процесу u_i.

2. Обґрунтування оптимального інтервалу дискретизації випадкового процесу в часі t.

3. Адаптація шкали квантування щодо нестаціонарності перетворюваних процесів та змінності інших факторів, що впливають на продуктивність аналого-цифрового перетворення.

4. 2. Етап вторинного перетворення послідовності. Обґрунтування ефективності методів вирівнювання статистичних характеристик

На другому етапі генерації послідовностей випадкових даних здійснюється вирівнювання статистичних характеристик. Серед доказово ефективних методів цього вирівнювання для систем захисту інформації є метод вибірки рівноймовірних комбінацій (von Neuman-Elias-Рябко-Мачикиної) [27–29] та метод кодової оброби (Santha-Vazirani) [30, 31].

Сутність *методу вибірки рівноймовірних комбінацій* полягає в наступному [27–29].

Послідовність X розбивається на відрізки довжиною n, які представляють собою певні комбінації із множини всіх можливих X_k^n у кількості 2^n. Перетворення X_k^n у відрізки, з яких формуватиметься результуюча послідовність Y, здійснюється за наступним правилом (табл.1).

Таблиця 1

Таблиця розподілу комбінацій X_k^n за ознакою рівної ваги wt

Вага комбінації wt	Комбінації $X_{k,wt}^n$ ваги wt	Кількість комбінацій $X_{k,wt}^n$
wt=0	$X_{1,0}^n$	1
wt=1	$X_{2,1}^n, X_{3,1}^n, \ldots, X_{n,1}^n, X_{n+1,1}^n$	n
wt=2	$X_{n+2,2}^n, X_{n+3,2}^n, \ldots, X_{n+\frac{n(n-1)}{2},2}^n, X_{n+1++\frac{n(n-1)}{2},2}^n$	$\frac{n(n-1)}{2}$
…….		

wt	$X_{wt}^{n}\sum_{b=0}^{wt-1}C_n^b+1, X_{wt}^{n}\sum_{b=0}^{wt-1}C_n^b+1,\ldots, X_{wt}^{n}\sum_{b=0}^{wt}C_n^b-1, X_{wt}^{n}\sum_{b=0}^{wt}C_n^b$	$C_n^{wt}=\frac{n!}{wt!(n-wt)!}$
…….		
wt=*n*–2	$X_{n-2}^{n2^n-n-\frac{n(n-1)}{2}-1}, X_{n-2}^{n2^n-n-\frac{n(n-1)}{2}},\ldots, X_{n-2}^{n2^n-n-3}, X_{n-2}^{n2^n-n-2}$	$\frac{n(n-1)}{2}$
wt=*n*–1	$X_{n-1}^{n2^n-n-1}, X_{n-1}^{n2^n-n},\ldots, X_{n-1}^{n2^n-2}, X_{n-1}^{n2^n-1}$	*n*
wt=*n*	$X_n^{2^n}$	1

Множина всіх X_k^n розділяється на підмножини комбінацій $X_{k,wt}^n$ за ознакою рівної ваги *wt*, *wt*=0÷*n*. Із кожної підмножини відбираються комбінації $X_{k,wt}^n$ так, щоб кількість була кратною деякому $2^{k'}$, де *k'* – натуральне число. Оскільки розподіл комбінацій $X_{k,wt}^n$ за вагою *wt* підпорядкований біноміальному закону, то *k* обирається за формулою′

$$k' = k_{wt} = \left\lceil \log_2 C_n^{wt} \right\rceil. \tag{4}$$

Відібраним комбінаціям ставляться у відповідність комбінації двійкових знаків $Y_l^{k'_{wt}}$, *l*=1, 2, 3,…, $2^{k'_{wt}}$, з яких формується вихідна послідовність *Y*.

Очевидно, що якщо послідовність *X* розподілена за бернуллiївським законом, то *Y* має бути ідеально випадковою послідовністю з рівноймовірним розподілом. При цьому відносно не складно може бути розрахованою і швидкість цього перетворення з використанням теореми Муавра-Лапласа, прирівнюючи цю швидкість до ймовірностей появи рівноймовірних комбінацій $X_{k,wt}^n$, яким присовуються вихідні комбінації $Y_l^{k'_{wt}}$. Наприклад, для *n*=2 швидкість перетворення визначатиметься формулою:

$$R = \frac{1}{\sqrt{2p(1-p)}}\phi\left(\frac{1-2p}{\sqrt{2p(1-p)}}\right), \tag{5}$$

де $\phi(x)=\frac{1}{\sqrt{2\pi}}e^{\frac{x^2}{2}}$ – табульована функція Гауса; *p* – імовірність одного з двійкових знаків послідовності *X*.

Реальні ж джерела мають далеко не бернуллiївський розподіл, а тому якою буде ефективність цього методу статистичного вирівнювання для реальних джерел є невідомою. Швидкість перетворення також може бути іншою ніж за-

значено формулою (5). Тому цей метод для реальних джерел вимагає окремих досліджень та експериментів. Зазначені недоліки усунені в методів генерації послідовностей випадкових даних з кодовою обробкою.

Сутність *методу кодової оброби* полягає в наступному [30, 31].

Послідовність X розбивається на відрізки довжиною n, кількість комбінацій яких складає 2^n. Перетворення X у Y_l^m, l=1, 2,…, 2^m, з яких формуватиметься результуюча послідовність Y, здійснюється за наступним правилом (рис. 3).

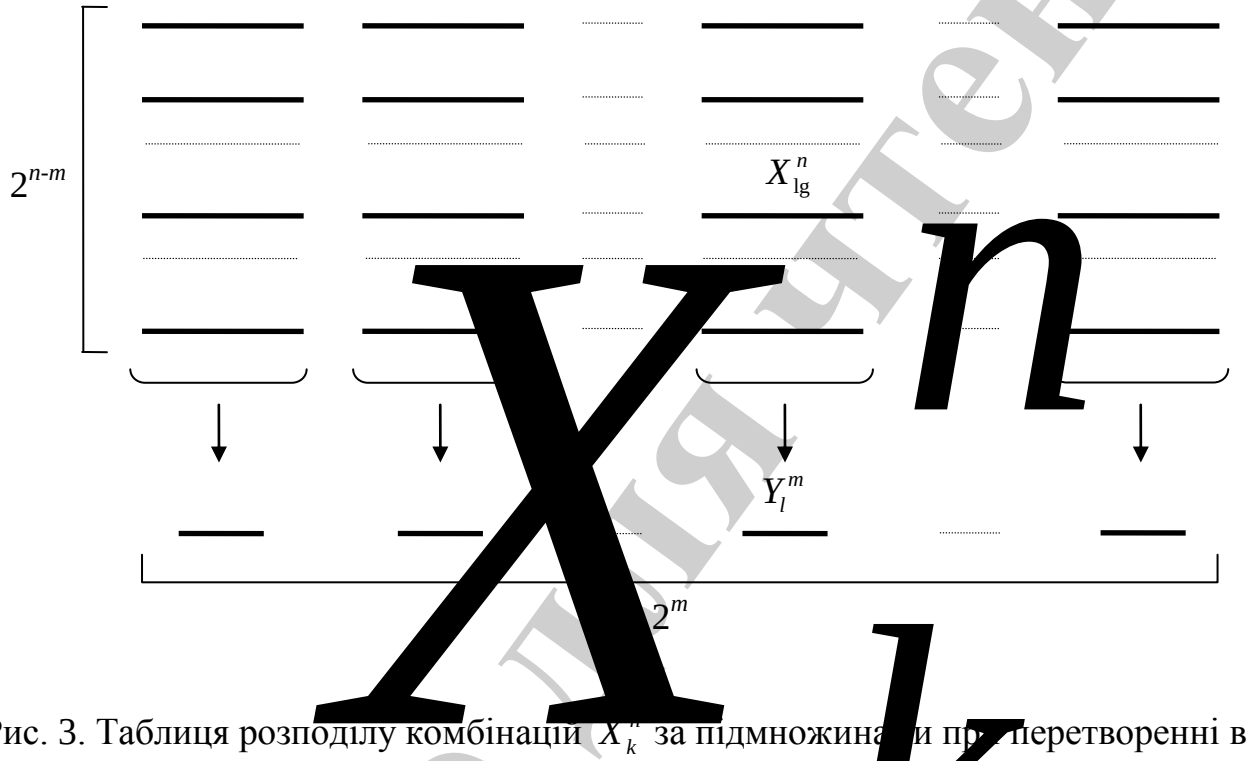

Рис. 3. Таблиця розподілу комбінацій X_k^n за підмножинами при перетворенні в Y_l^m з кодовою обробкою

Множина комбінацій X_k^n розділяється на підмножини однакового об'єму так, щоб кількість складала 2^m (m<n). Кожній підмножині ставиться у відповідність певна комбінація Y_l^m з яких формується вихідна послідовність Y.

Очевидно, що комбінації $X_{\lg}^n$ можна розподілити за підмножинами таким чином, що в середньому вихідна Y матиме більшу близькість до рівноймовірного розподілу ніж X. При цьому швидкість перетворення R не є ймовірнісною величиною як в методі вибірки рівноймовірних комбінацій, а жорстко визначається параметрами m та n. Вона дорівнює:

$$R = \frac{m}{n}. \qquad (6)$$

Слід зазначити, що кодова обробка може бути реалізованою з використанням лінійного завадостійкого коду, та зводиться при цьому до відносно нескла-

дної операції множення X_k^n на перевірочну матрицю, або на поліном для циклічного коду [32]. Завдання пошуку ефективних кодів за критерієм максимуму продуктивності (2) з заданою якістю вихідної послідовності збігається з пошуком ефективних кодів для забезпечення максимуму завадостійкості [31]. При цьому показано, що з використанням для кодової оброки лінійних кодів можна досягти досить високої ефективності, яка забезпечується формуванням великих об'ємів підмножин $\left\{ X_{l1}^n, X_{l2}^n, \ldots, X_{\lg}^n, \ldots, X_{l2}^{n\,n-m} \right\}$, де l=1, 2,…, 2^m.

В роботі [31] наведено доведення того, що таке перетворення забезпечує ефективність вирівнювання статистичних характеристик не тільки для бернуллівського розподілу ймовірностей. На відміну від методу вибірки рівно ймовірних комбінацій (von Neuman-Elias-Рябко-Мачикиної) ефективність вирівнювання цим методом забезпечується і для слабо випадкового розподілу, який враховує статистичні зв'язки поміж даними в послідовності [30].

Реальні ж джерела послідовностей випадкових даних є далеко не бернуллівські. Слабо випадковість також передбачає стаціонарність джерела, яка не завжди має місце для реальних джерел.

Таким чином, проведено аналіз методів вирівнювання статистичних характеристик послідовностей випадкових даних. Вони мають наступну ефективність:

1. Метод вибірки рівно ймовірних комбінацій (von Neuman-Elias-Рябко-Мачикиної) [27–29] є доказово ефективним для бернуллівського розподілу перетворюваних послідовностей. Швидкість перетворення є асинхронною та залежить від статистичних властивостей послідовності.

2. Метод кодової обробки (Santha-Vazirani) [30, 31] є доказово ефективним не тільки для бернуллівского, а й для слабо випадкового розподілу перетворюваних послідовностей. Швидкість перетворення є синхронною та повністю визначається сталими параметрами вхідних та вихідних комбінацій.

5. Результати дослідження шляхів підвищення продуктивності генерації випадкових послідовностей

5. 1. Обґрунтування оптимальної шкали квантування динамічного діапазону випадкового процесу

Реальні шумові процеси характеризуються досить високим ступенем невизначеності, яку для забезпечення максимуму ентропії на відлік при перетворенні процесу потрібно конвертувати у випадкову послідовність з мінімальними втратами.

Нехай для простоти випадковий процес, що використовується для перетворення у випадкову послідовність, є стаціонарним. Нехай задано ансамбль реалізацій цього випадкового процесу, що виражається щільністю розподілу ймовірностей □(*u*) з заданими математичним сподіванням *a* та середньоквадратичним відхиленням □. Для забезпечення максимуму ентропії

$$H(X) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} p(X_k^n) \log_a \frac{1}{p(X_k^n)} \qquad (7)$$

необхідне виконання умови рівноймовірності комбінацій знаків X_k^n [26, 33, 34]. Зазначена рівність ймовірностей зводиться до забезпечення рівності площ під кривою щільності розподілу на рис. 4, обмежених градацією шкали динамічного діапазону u.

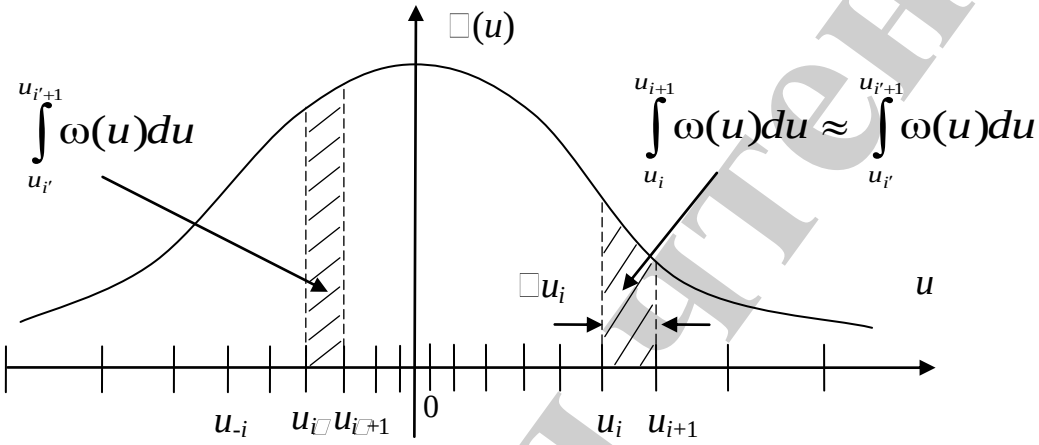

Рис. 4. Щільність розподілу ймовірностей випадкової неперервної величини u та зображення прикладу шкали, що забезпечує рівність ймовірностей при аналого-цифровому перетворенні – площ поміж поділками

Якщо n обмежене та $N=2^{n-1}$, то можна використати відповідність ймовірностей комбінацій X_k^n та того, що значення u□$[u_i; u_{i+1}[$:

$$p(X_k^n) = p_i(X^n) = p(u_i \le u < u_{i+1}) = \\ = \int_{u_i}^{u_{i+1}} \omega(u)du = p(u_i). \qquad (8)$$

Шкала квантування може бути знайденою виходячи з виконання умови рівності інтегралів:

$$\int_0^{u_{\pm 1}} \omega(u)du \approx \int_{u_{\pm 1}}^{u_{\pm 2}} \omega(u)du \approx \ldots \approx \int_{u_{\pm i}}^{u_{\pm (i+1)}} \omega(u)du \approx \ldots \qquad (9)$$

Таким чином, на першому етапі генерації оптимізація шкали квантування динамічного діапазону випадкового процесу зводиться до забезпечення максимально можливої величини N та виконання умови (9).

1. Максимум величини N забезпечує максимум довжини n кодової комбінації X_k^n, отриманої з одного відліку при аналого-цифровому перетворенні.

2. Умова (9) забезпечує рівність ймовірностей $p(X_k^n)$ та, відповідно, максимум ентропії, розрахованої на один розряд випадкової комбінації X^n за співвідношенням (7).

5. 2. Обґрунтування оптимального інтервалу дискретизації випадкового процесу в часі

Зменшення інтервалу дискретизації неперервного процесу приводить до збільшення швидкості зчитування миттєвих значень – відліків. Також відомо, що зменшення цього інтервалу для будь-якого випадкового неперервного процесу приводить до зменшення різниці поміж сусідніми відліками та збільшенням статистичних зв'язків. Тому обґрунтування інтервалу дискретизації випадкового процесу в часі полягає у обґрунтуванні певної мінімальної величини $\Delta t_{\min}$, яка б не приводила до зниженні продуктивності генерації. Ця величина і буде оптимальною за критерієм максимуму продуктивності (2). Іншими словами вона має бути такою, щоб відліки зчитування миттєвих значень перетворюваного процесу ще не мали статистичної залежності, або ця залежність буде не суттєвою з врахуванням другого етапу перетворення. Очевидно, що забезпечення статистичної незалежності відліків дозволить генерувати послідовність статистично незалежних випадкових даних з досить високою ентропією.

На обирання інтервалу $\Delta t_{\min}$ мають вплив два фактори:

1. Схемо-технічні обмеження зі швидкодії аналого-цифрових перетворювачів.

2. Обмеження перетворюваного процесу $u(t)$ за його спектральними та статистичними характеристиками.

Перший фактор пов'язаний з наявністю власних ємності та індуктивності в електронній елементній базі, які в сучасній схемотехніці мінімізуються шляхом підвищення ступеня інтеграції мікросхем, використанням високо провідних матеріалів, тощо. Так, на сьогоднішній день прикладом швидкодіючих засобів є сучасні засоби спектрального аналізу, наприклад, відомої в світі фірми Rohde&Schwarz типу R&S®FSW85, R&S®FSWP50, R&S®FSMR50. Вони надають можливість вимірювання та аналізу неперервних процесів в спектрі до 50□85 ГГц.

Слід зазначити, що це є пригранічними частотами електромагнітного поля, що супроводжується електричними струмами. Застосування оптичної електроніки в діапазоні $10^{12} \div 10^{15}$ Гц, де носієм виступатиме не електричний струм, а фотон світла, дозволить суттєвим чином збільшити зазначену швидкість. Ці перспективні способи розглянуті в роботах [12–17] забезпечують отримання випадкових послідовностей, що відносяться до нового покоління та засновані на квантово-механічній теорії.

Другий фактор, що обмежує мінімізацію інтервалу зчитування, – це частота Найквіста випадкового процесу та статистична залежність миттєвих значень відліків [26]. Вже було зазначено, що зчитування процесу зі швидкістю, що пе-

ревищує частоту Найквіста, приведе до зменшення різниці між миттєвими значеннями відліків, та тим самим до збільшення між ними статистичного зв'язку.

Таким чином, оптимальність інтервалу дискретизації випадкового процесу в часі $\Delta t_{\min}$ не є однозначною. Її обґрунтування може здійснюватись з трьох точок зору:

1. З забезпеченням максимуму конвертування невизначеності на етапі перетворення неперервного випадкового процесу у послідовність випадкових даних на максимальних швидкостях без врахування наявності в послідовності можливих статистичних дефектів. При цьому усунення останніх передбачається на 2 етапі генерації – етапі вирівнювання статистичних характеристик, яке здійснюється за рахунок зниження швидкості.

2. З забезпеченням конвертування максимуму невизначеності неперервного процесу у вихідну послідовність за умови наявності в ній мінімуму або повної відсутності статистичних дефектів. Підвищення швидкості зчитування не повинно приводити до зростання або появи цих дефектів. При цьому вирівнювання статистичних характеристик послідовності стає несуттєвим або і зовсім непотрібним [35].

3. З забезпеченням конвертування максимуму невизначеності неперервного процесу у вихідну послідовність з оптимізацією узгодження швидкостей на 1 та 2 етапах генерації.

Щодо першої точки зору інтервал зчитування може бути знайденою з використанням теореми Котельникова [26], яка стверджує що будь-який фінітний за часом та за спектром аналоговий сигнал можна повністю представити у виді $2\Delta F\Delta t$ відліків, де ΔF – ширина спектру сигналу. При цьому

$$\Delta t_{\min 1} = \frac{1}{2\Delta F}. \qquad (10)$$

Так, наприклад, для n=8 та за умови оптимальної шкали динамічного діапазону (9). При ширині спектру перетворюваного шумового процесу 250 кГц можна отримати послідовність випадкових даних з інтервалом зчитування 2 мкс та продуктивністю приблизно 128 Мбіт/с.

З другої точки зору $\Delta t_{\min 2}$ має обиратись емпіричними методами за допомогою статистичного тестування неперервного процесу. Це доцільно здійснювати шляхом прийняття деякого базового значення інтервалу, наприклад $\Delta t'_{\min 2}=\Delta t_{\min 1}$, та поступового наближення його до значення $\Delta t_{\min 2}=\Delta t'_{\min 2}>\Delta t_{\min 1}$. При цьому має виконуватися умова статистичної незалежності відліків. Такий інтервал забезпечує низьку швидкість генерації та має нижню межу:

$$\Delta t_{\min 2} \geq \frac{1}{\Delta F}. \qquad (11)$$

Так, для умов попереднього прикладу інтервал зчитування зросте та, відповідно, швидкість генерації спаде в понад 2 рази, а тому продуктивність зме-

ншиться та не перевищуватиме 64 Мбіт/с.

Щодо третьої точки зору інтервал $\Box t_{min3}$ знаходиться таким, щоб в сукупності зі швидкістю статистичного вирівнювання R виконувався критерій генерації послідовностей випадкових даних (2).

При цьому з усіх трьох точок зору інтервали зчитування мають знаходитись у співвідношенні:

$$\Box t_{min1} < \Box t_{min3} < \Box t_{min2}. \quad (12)$$

Слід також зазначити, що інтервал зчитування не визначає остаточну продуктивність джерела. Для забезпечення потрібної якості отримана від перетворення фізичного шумового процесу послідовність підлягає вирівнюванню статистичних характеристик, яке буде пов'язане з втратами швидкісних показників генерації.

5. 3. Обґрунтування вибору ефективного методу щодо вирівнювання статистичних характеристик для систем захисту інформації

Одним з головних питань будь-якої системи захисту інформації є гарантування безпеки, яке в частині використання генераторів послідовностей випадкових даних вимагає від них заданої статистичної надійності. В свою чергу, потрібну надійність можуть гарантувати лише доказово ефективні методи.

На відміну від методу вибірки рівноймовірних комбінацій (von Neuman-Elias-Рябко-Мачикиної) [27–29] метод кодової обробки (Santha-Vazirani) [30, 31] забезпечує доказову ефективність для слабо випадкового розподілу. Слабо випадковий розподіл враховує зав'язок кожного розряду послідовності випадкових даних з його передісторією, яка зменшує ступінь невизначеності та з певним ступенем достовірності дозволяє відгадування даних. Це є суттєвим фактором для систем захисту інформації, які повинні забезпечувати безпеку інформаційних ресурсів.

Практично всі практичні джерела мають слабо випадковий розподіл. Тому для вирівнювання статистичних характеристик доцільним є використання методу кодової обробки (Santha-Vazirani) як доказово ефективного. Ефективність цього методу зручно показати за допомогою рис. 5. В ньому зазначені графіки залежності ентропії вихідної послідовності від ентропії вхідної для теоретичного максимуму та практичної ефективності кодової обробки, а також за відсутності кодової обробки.

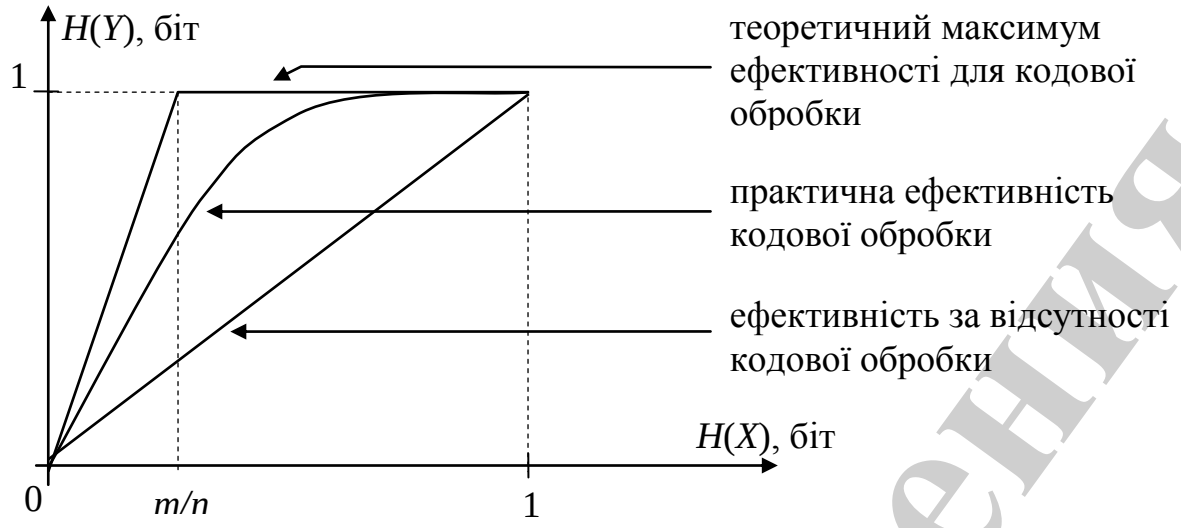

Рис. 5. Графічне зображення залежності ентропії вихідної послідовності від ентропії вхідної для теоретичного максимуму та практичної ефективності кодової обробки, а також за відсутності кодової обробки

Метод кодової обробки має відносно невелику складність реалізації. Наприклад, використання лінійного коду дозволяє здійснення кодової оброки шляхом нескладної операції множення відрізків вхідної послідовності на перевірочну матрицю коду, або на поліном для циклічного коду. Покращення ефекту вирівнювання статистичних характеристик за критерієм максимуму продуктивності (2), досягається шляхом розширення коду та використанням досконалих кодів при кодовій обробці [34].

5. 4. Обґрунтування способів адаптації параметрів перетворення щодо нестаціонарності перетворюваних процесів

За умови нестаціонарності перетворюваних процесу та змінності інших факторів, що впливають на продуктивність генерації, необхідна адаптація параметрів на всіх етапах перетворення. Адаптація потрібна під час функціонування засобу генерації, а тому можлива шляхом застосування зворотних зв’язків з потрібним коригуванням параметрів, як показано на рис. 6.

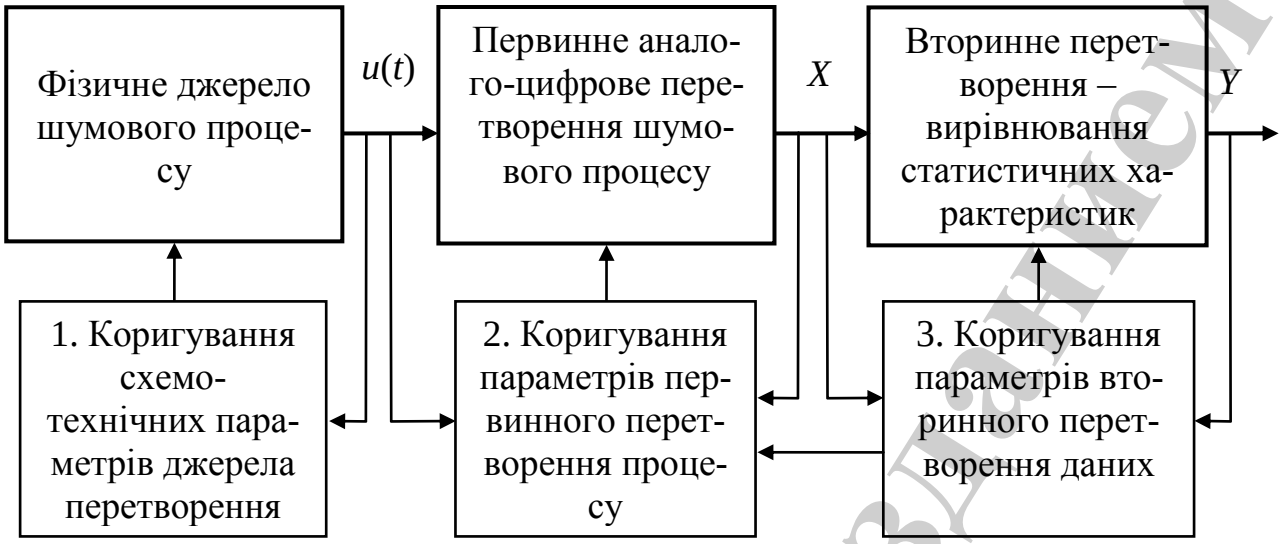

Рис. 6. Схема двох етапної генерації випадкових послідовностей від нестаціонарного фізичного джерела з адаптацією параметрів аналого-цифрового перетворення та вирівнювання статистичних характеристик

1. Коригування схемо-технічних параметрів джерела здійснюється на основі статистичного аналізу виробленого шумового процесу $u(t)$ шляхом адаптації (підсилення або послаблення) сигналу до ознак стаціонарності. Для цього може бути використаним правило Слуцького, яке має вид:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T R(\tau)\mathrm{d}\tau = 0, \qquad (13)$$

де $R(\square)$ – функція кореляції шумового процесу:

$$R(\tau) = \frac{1}{T}\int_0^T u(t)u(t-\tau)\mathrm{d}\tau. \qquad (14)$$

2. При коригуванні параметрів на першому етапі аналого-цифрового перетворення шумового процесу вирішується два завдання:

– на основі статистичного аналізу шумового процесу $u(t)$ здійснюється формування та адаптація шкали аналого-цифрового перетворення до щільності розподілу ймовірностей;

– на основі статистичного тестування послідовності X здійснюється коригування кількості рівнів квантування, що приводитиме до укрупнення, або роздрібнення шкали аналого-цифрового перетворення [36, 37].

3. При коригуванні параметрів на другому етапі вирівнювання статистичних характеристик послідовності X також вирішується два завдання:

– на основі статистичного тестування послідовності X здійснюється вибір коду для виконання кодової обробки, що має забезпечити потрібну якість результуючої послідовності Y;

– на основі статистичного тестування послідовності Y здійснюється коригування інтервалу дискретизації перетворюваного випадково процесу в часі та адаптація параметрів кодової обробки до забезпечення потрібної якості Y [36, 37].

6. Обговорення результатів досліджень шляхів підвищення продуктивності випадкових послідовностей

Підвищення продуктивності генераторів випадкових послідовностей, що зумовлено потребами сучасних систем захисту інформації, вимагає комплексного вирішення на обох етапах генерації.

Таким чином на першому етапі генерації за критерієм максимуму продуктивності запропоновано:

– оптимізацію шкали квантування динамічного діапазону перетворюваного випадкового процесу;

– оптимізацію інтервалу дискретизації випадкового процесу в часі.

Оптимізація шкали квантування зводиться до забезпечення максимально можливої величини рівнів квантування N та виконання умови (8) – рівності площ за поділками шкали під кривою щільності розподілу ймовірностей. Збільшення N при перетворенні шумового процесу $u(t)$ приводить до збільшення розрядності n ($n \geq \log_2(2N)$) комбінацій X_k^n, k=1, 2, 3, … 2^n, а оптимізація шкали до рівноймовірності цих комбінацій для всіх k. Так, при збільшенні величини N вдвічі, наприклад, з 2048 до 4096, розрядність вихідної комбінації n зросте з 10 до 11. При цьому швидкість генерації, а при збереженні рівноймовірності X_k^n і продуктивність зросте в 1,1 раза.

Оптимізація інтервалу дискретизації випадкового процесу в часі $\geq t_{\min}$ не є однозначною. При її обґрунтуванні використано три точки зору:

– це забезпечення максимуму швидкості зчитування, при збільшенні якої продуктивність не зростатиме;

– це забезпечення максимуму швидкості зчитування, при якій ще відсутні статистичні зв’язку між відліками;

– це забезпечення швидкості зчитування між вище зазначеними максимумами, в залежності від того, з якою ефективністю здійснюватиметься вирівнювання статистичних характеристик.

Очевидно, що при зменшенні інтервалу дискретизації в часі завдяки появі статистичних зв’язків між відліками зменшуватиметься ентропія $H(X)$. Тобто не зважаючи на високу продуктивність первинного перетворення, послідовність X може вироблятись з високою швидкістю, але з недостатньою якістю. Тому виникає необхідність підвищення цієї якості, що здійснюється шляхом вирівнювання статистичних характеристик.

На другому етапі з метою вирівнювання статистичних характеристик запропоновано використання методу кодової обробки. Кодова обробка завдяки

певному доказово ефективному перетворенню, що пов'язане зі зниженням швидкості, дозволяє підвищити статистичну якість послідовності.

Проведено оцінювання ефективності кодової обробки для деяких кодів, а саме кодів з перевірки на парність, Хемінга, БЧХ, Голея. Ефективність виражається швидкістю перетворення та залежністю ентропій після кодової обробки та до кодової обробки. Результати оцінювання представлені в табл. 2.

Таблиця 2

Залежності ентропій після та до кодової обробки з використанням кодів з перевірки на парність, Хемінга, БЧХ, Голея

Відсутність кодової обробки	Кодова обробка з використанням кодів					
	БЧХ (31,21)	Голея (24,12)	Перев. на парн.(4,3)	Перев. на парн. (11,10)	Хемінга (15,11)	Хемінга. (63,57)
Швидкість кодової обробки: $R=m/n$						
1	0,32	0,5	0,25	0,09	0,27	0,095
$H(X)$, біт	Ентропія $H(Y)$, біт					
0,011	0,035	0,023	0,037	0,081	0,042	0,116
0,045	0,140	0,091	0,140	0,287	0,164	0,410
0,081	0,248	0,162	0,230	0,460	0,283	0,633
0,141	0,426	0,283	0,372	0,680	0,462	0,858
0,194	0,567	0,387	0,499	0,805	0,594	0,948
0,242	0,678	0,480	0,589	0,881	0,694	0,982
0,286	0,765	0,562	0,662	0,927	0,771	0,994
0,327	0,832	0,635	0,722	0,956	0,829	0,998
0,365	0,882	0,700	0,770	0,973	0,874	0,999
0,402	0,919	0,755	0,812	0,985	0,907	□1
0,436	0,946	0,803	0,847	0,991	0,933	
0,468	0,965	0,844	0,875	0,995	0,952	
0,610	0,997	0,961	0,958	0,999	0,999	
0,722	0,999	0,994	0,987	□1	□1	
0,811	□1	0,999	0,991			
0,881		□1	0,994			
0,971			0,999			

Значення табл. 2 мають графічне представлення на рис. 7.

Аналогічно теоретичному проведено експериментальне дослідження ефективності кодової обробки на прикладі коду Хемінга (63,57). Дослідження ентропій здійснювалось з використанням тесту Маурера [36]. Отримані результати представлені в табл. 3 та у вигляді графіку на рис. 7, що виділений жирною лінією.

Таблиця 3

Залежності експериментально отриманих ентропій після та до кодової обробки на прикладі коду Хемінга (63, 57)

$H(X)_{експ}$,біт	0,010	0,039	0,070	0,120	0,166	0,207	0,247	0,349	0,411
$H(Y)_{експ}$,біт	0,118	0,398	0,604	0,807	0,888	0,916	0,926	0,931	0,930

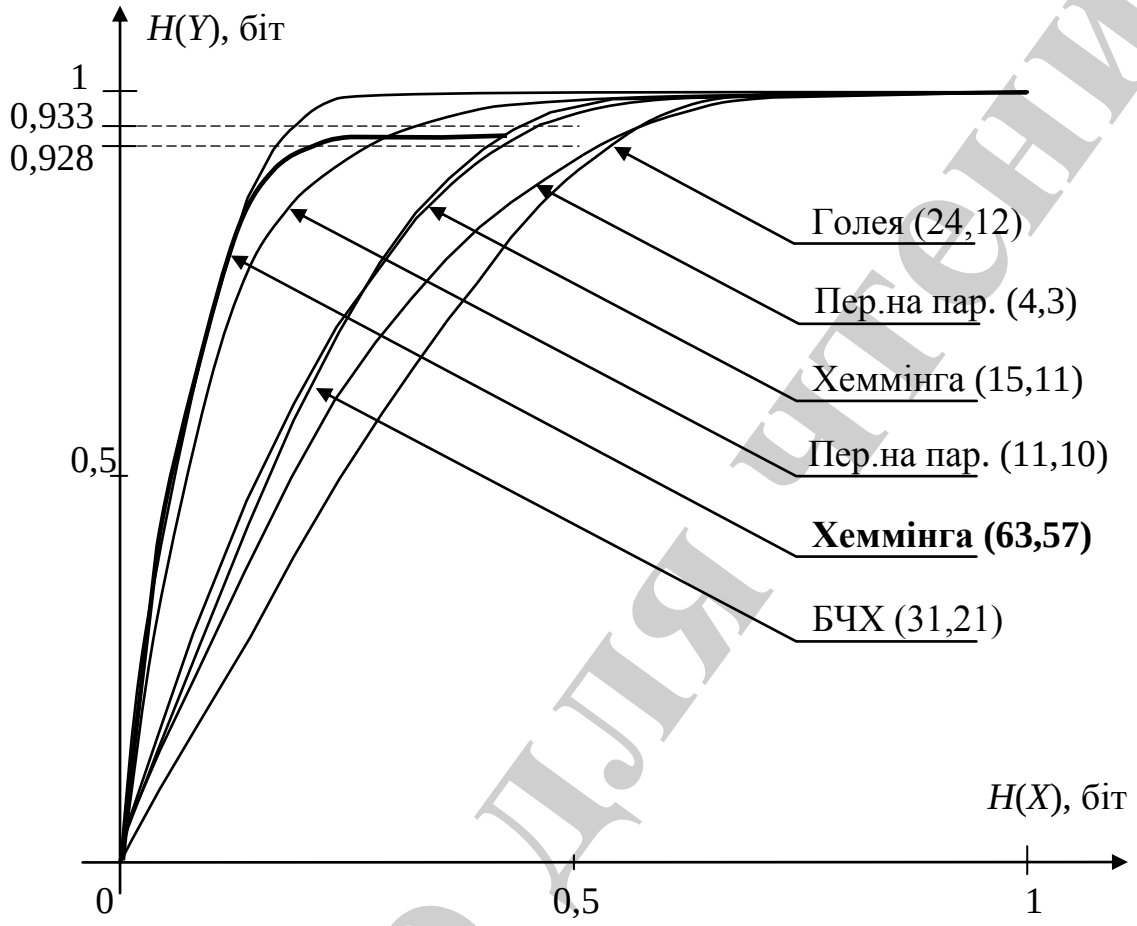

Рис. 7. Графік залежності ентропій після та до кодової обробки з використанням кодів з перевірки на парність, Хемінга, БЧХ та Голея

Як видно з графіку, результати теоретичних та практичних досліджень кодової обробки для коду Хемінга (64, 57) майже співпадають. Відмінності, що мають місце у верхній області значень $H(Y)$, зумовлені умовами тестування. Наведені на осі $H(Y)$ значення ентропій 0,933 біт та 0,928 біт є межами щодо позитивного тестування, які визначені ступенем довіри. Тобто, якщо результат тестування попадає в зазначені межі, то досліджена послідовність вважається достатньо випадковою, що відповідає теоретичному 1 біт ентропії.

В разі нестаціонарності перетворюваного випадкового процесу підвищення продуктивності потребує адаптацію параметрів перетворення на обох етапах перетворення. Вона має здійснюватись за допомогою зворотних зв’язків наступним чином (рис. 6):

– коригування схемо-технічних параметрів джерела (підсилення, послаблення сигналу) з метою виділення стаціонарної шумової складової з перетворюваного процесу;

– коригування та адаптація шкали квантування та інтервалу зчитування щодо залишкової нестаціонарності джерела при перетворенні шумового процесу на першому етапі генерації;

– коригування та адаптація параметрів вирівнювання статистичних характеристик щодо недостатності статистичної якості та нестаціонарності послідовності на другому етапі генерації.

Всі види коригувань на етапах генерації мають здійснюватись на основі статистичного тестування вихідних процесів або послідовностей даних [36, 37].

7. Висновки

1. Запропоновано оптимізацію чинників, які дозволяють підвищити продуктивність генерації послідовностей випадкових даних від фізичних джерел. Оптимізацію чинників здійснено з використанням двохетапного представлення генерації: аналого-цифрового перетворення шумових процесів та вирівнювання статистичних характеристик отриманої послідовності. На етапі аналого-цифрового перетворення такими чинниками є шкала квантування динамічного діапазону та інтервал дискретизації перетворюваного випадкового процесу в часі. Обґрунтовано умову, якій має відповідати оптимальна шкала та межі для оптимального інтервалу дискретизації перетворюваного випадкового процесу в часі. На відміну від шкали, оптимізація інтервалу здійснюється за критерієм максимуму продуктивності не на першому етапі аналого-цифрового перетворення, а з врахуванням ефективності вирівнювання статистичних характеристик на другому етапі генерації.

2. Для вирівнювання статистичних характеристик обґрунтовано використання методу кодової обробки (Santha-Vazirani), який є доказово ефективним методом для слабо випадкових джерел. Про виборі ефективних методів, що підвищують ентропію випадкової послідовності, окрім зазначеного також розглядався метод вибірки рівно ймовірних комбінацій (von Neuman-Elias-Рябко-Мачикиної). Метод кодової обробки має відносно нескладну реалізацію з використанням лінійних кодів та зводиться до операції множення відрізків вхідної послідовності на перевірочну матрицю коду, або на поліном циклічного коду. Однак дослідження показали, що цей метод є доказово ефективним лише для бернуллііївського розподілу послідовності даних. Тому з точки зору вимог систем захисту інформації, для яких має бути виключеною можливість відгадування даних, був відхиленим. Покращення ефекту вирівнювання статистичних характеристик досягається шляхом розширення коду.

3. Для продуктивного отримання послідовностей випадкових даних від нестаціонарних фізичних джерел та з врахування змінності інших факторів, що впливають на продуктивність, запропоновані способи адаптації параметрів генерації. Вони можуть бути реалізованими на основі статистичного контролю виходів елементів генерації та коригування параметрів цих елементів посередництвом зворотних зв'язків.

Запропоновані оптимізація параметрів генерації випадкових послідовностей та способи їх адаптації до не стаціонарності фізичного джерела на практиці можуть надати можливість досягнення високих показників продуктивності. Вони є відносно нескладними щодо реалізації за допомогою сучасних техніки та технологій в масштабах реального часу та можуть бути ефективно використаними в реальних системах захисту інформації.

Література

1. Иващенко А. В., Сыпченко Р. П. Основы моделирования сложных систем на ЭВМ. Л.: ЛВВИУС, 1988. 272 с.
2. Молдавян Н. А. Проблематика и методы криптографии. СПб.: Издательство СПбГУ, 1998. 212 с.
3. Muramatsu J., Miyake S. Uniform Random Number Generation and Secret Key Agreement for General Sources by Using Sparse Matrices // Mathematics for Industry. 2017. P. 177–198. doi: https://doi.org/10.1007/978-981-10-5065-7_10
4. Wyner A. D. The Wire-Tap Channel // Bell System Technical Journal. 1975. Vol. 54, Issue 8. P. 1355–1387. doi: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
5. Коржик В. И., Яковлев В. А. Неасимптотические оценки эффективности кодового зашумления одного канала. М.: Проблемы передачи информации, 1981. С. 11–18.
6. Elliptic Curve Cryptography in Practice / Bos J. W., Halderman J. A., Heninger N., Moore J., Naehrig M., Wustrow E. // Lecture Notes in Computer Science. 2014. P. 157–175. doi: https://doi.org/10.1007/978-3-662-45472-5_11
7. Zhou H. Randomness and Noise in Information Systems. California Institute of Technology Pasadena, California 2013. 436 p.
8. An experimental implementation of oblivious transfer in the noisy storage model / Erven C., Ng N., Gigov N., Laflamme R., Wehner S., Weihs G. // Nature Communications. 2014. Vol. 5, Issue 1. doi: https://doi.org/10.1038/ncomms4418
9. Implementation of two-party protocols in the noisy-storage model / Wehner S., Curty M., Schaffner C., Lo H.-K. // Physical Review A. 2010. Vol. 81, Issue 5. doi: https://doi.org/10.1103/physreva.81.052336
10. Unfair Noisy Channels and Oblivious Transfer / Damgård I., Fehr S., Morozov K., Salvail L. // Lecture Notes in Computer Science. 2004. P. 355–373. doi: https://doi.org/10.1007/978-3-540-24638-1_20
11. Бобнев М. П. Генерирование случайных сигналов. М.: Энергия, 1971. 240 с.
12. Методы и средства генерации случайных битовых последовательностей / Торба А. А., Бобкова А. А., Горбенко Ю. И., Бобух В. А. под ред. И. Д. Горбенко. Харьков: Изд-во «Форт», 2012. 232 с.
13. Colbeck R., Renner R. Free randomness can be amplified // Nature Physics. 2012. Vol. 8, Issue 6. P. 450–453. doi: https://doi.org/10.1038/nphys2300

14. Full randomness from arbitrarily deterministic events / Gallego R., Masanes L., De La Torre G., Dhara C., Aolita L., Acín A. // Nature Communications. Vol. 4, Issue 1. doi: https://doi.org/10.1038/ncomms3654

15. Chung K.-M., Shi Y. Wu X. Physical randomness extractors: generating random numbers with minimal assumptions. URL: https://arxiv.org/pdf/1402.4797.pdf

16. Mironowicz P., Gallego R., Pawłowski M. Robust amplification of Santha-Vazirani sources with three devices // Physical Review A. 2015. Vol. 91, Issue 3. doi: https://doi.org/10.1103/physreva.91.032317

17. Robust device-independent randomness amplification with few devices / Brandao F. G. S. L., Ramanathan R., Grudka A., Horodecki K., Horodecki M., Horodecki P. et. al. // URL: https://arxiv.org/abs/1310.4544

18. Real-time fast physical random number generator with a photonic integrated circuit / Ugajin K., Terashima Y., Iwakawa K., Uchida A., Harayama T., Yoshimura K., Inubushi M. // Optics Express. 2017. Vol. 25, Issue 6. P. 6511. doi: https://doi.org/10.1364/oe.25.006511

19. Gurubilli P. R., Garg D. Random Number Generation and its Better Technique. Computer Science and Engineering Department, Thapar University, Patiala, 2010.

20. Elsherbeny M. N., Rahal M. Pseudo – Random Number Generator Using Deterministic Chaotic System // International Journal of Scientific & Technology Research. 2012. Vol. 1, Issue 9. P. 95–97.

21. Kozierski P., Lis M., Królikowski A. Parallel uniform random number generator in FPGA // Poznan University of Technology, Academic Journals: Computer Application in Electrical Engineering. 2014. Vol. 12. P. 399–406.

22. 54 Gbps real time quantum random number generator with simple implementation / Yang J., Liu J., Su Q., Li Z., Fan F., Xu B., Guo H. // Optics Express. 2016. Vol. 24, Issue 24. P. 27475. doi: https://doi.org/10.1364/oe.24.027475

23. Minimal-post-processing 320-Gbps true random bit generation using physical white chaos / Wang A., Wang L., Li P., Wang Y. // Optics Express. 2017. Vol. 25, Issue 4. P. 3153. doi: https://doi.org/10.1364/oe.25.003153

24. Chaotic laser based physical random bit streaming system with a computer application interface / Shinohara S., Arai K., Davis P., Sunada S., Harayama T. // Optics Express. 2017. Vol. 25, Issue 6. P. 6461. doi: https://doi.org/10.1364/oe.25.006461

25. Argyris A., Pikasis E., Syvridis D. Gb/s One-Time-Pad Data Encryption With Synchronized Chaos-Based True Random Bit Generators // Journal of Lightwave Technology. 2016. Vol. 34, Issue 22. P. 5325–5331. doi: https://doi.org/10.1109/jlt.2016.2615870

26. Баскаков С. И. Радиотехнические цепи и сигналы. М.: Высшая школа, 1988. 448 с.

27. von Neuman J. Various Techniques Used in Connection with Random Digits // Monte Carlo Method, Applied Mathematics. 1951. P. 36–38.

28. Elias P. The Efficient Construction of an Unbiased Random Sequence // The Annals of Mathematical Statistics. 1972. Vol. 43, Issue 3. P. 865–870. doi: https://doi.org/10.1214/aoms/1177692552

29. Рябко Б. Я., Мачикина Е. П. Эффективное преобразование случайных последовательностей в равновероятные и независимые // Проблемы передачи информации. 1998. Т. 35, № 2. С. 23–28.

30. Santha M., Vazirani U. V. Generating quasi-random sequences from semi-random sources // Journal of Computer and System Sciences. 1986. Vol. 33, Issue 1. P. 75–87. doi: https://doi.org/10.1109/sfcs.1984.715945

31. Іванченко С. О., Паршуков С. С. Обґрунтування методу генерації випадкових послідовностей з кодовою обробкою для криптографічних систем захисту інформації // Спеціальні телекомунікаційні системи та захист інформації: Тематичний випуск “Математичні методи прикладної криптографії”. 2007. Вип. 1 (13). С. 152–155.

32. Іванченко С. О., Зайцев О. Д. Метод високопродуктивного перетворення шумових сигналів у випадкову послідовність // Спеціальні телекомунікаційні системи та захист інформації. 2009. Вип. 2 (16). С. 140–144.

33. Галлагер Р. Г. Теория информации и надежная связь. М.: Советское радио, 1974. 720 с.

34. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.

35. Murry H. F. A General Approach for Generating Natural Random Variables // IEEE Transactions on Computers. 1970. Vol. C-19, Issue 12. P. 1210–1213. doi: https://doi.org/10.1109/t-c.1970.222860

36. Maurer U. Provable Security in Cryptography // Diss. ETH No 9260. 1990. P. 86–93.

37. A statistical test suite for random and pseudorandom number generators for cryptographic applications / Bassham L. E., Rukhin A. L., Soto J., Nechvatal J. R., Smid M. E., Barker E. B. et. al. National Institute of Standards and Technology, 2010. 131 p. doi: https://doi.org/10.6028/nist.sp.800-22r1a