10.46299/ISG.2022.MONO.TECH.4.2.7

2.7 Недерміновані генератори випадкових бітів на основі стандарту ISO/IEC 18031:2005

Міжнародний стандарт ISO/IEC 18031:2005 – Information technology – Security techniques – Random bit generation (Інформаційні технології – Методи захисту – Генерація випадкових бітів) [202] встановлює обов'язкові вимоги, яких необхідно дотримуватися при розробці генераторів випадкових бітів для криптографічних застосувань.

Ці криптографічні застосування включають наступне [203]:

- випадкові ключі і значення ініціалізації для шифрування;
- випадкові особові ключі для алгоритмів цифрового підпису;
- випадкові значення, які використовуються в механізмах аутентифікації об'єктів;
- генерація випадкових PIN, паролів та ін.

Стандарт ISO/IEC 18031:2005 визначає два типи генераторів: недерміновані і детерміновані генератори випадкових бітів [202,203].

Недетермінований генератор випадкових бітів – НГВБ (non deterministic random bit generator – NRBG) – це механізм генерації випадкових бітів, який використовує джерело ентропії (джерело невизначеності) для генерації випадкового потоку бітів (випадкових послідовностей).

Детермінований генератор випадкових бітів – ДГВБ (deterministic random bit generator – DRBG) – це механізм генерації бітів, який використовує детерміновані алгоритми, такі як криптографічні алгоритми, на джерелі ентропії для генерації випадкового потоку бітів (випадкових послідовностей). У цьому типі генерації бітів використовується особливі вхідні дані (початкові значення) і, можливо, деякі необов'язкові вхідні дані, які можуть (чи не можуть) бути загальнодоступними.

Необхідні властивості випадковості можливо досліджувати, використовуючи приклад підкидання монети. Результатом кожного підкидання монети є:

1. **Непередбачуваність**: перед підкиданням невідомо, якою стороною приземлиться монета, «орлом» або «ешкою». Також, якщо підкидання монети тримається в таємниці, то неможливо визначити результат підкидання, навіть за умови, якщо відомі наступні результати підкидання;

2. **Незміщеність:** кожен потенційний результат має одну і ту ж імовірність появи. При рівній імовірності результатів ентропія (непередбачуваність) результатів експерименту буде максимальною;

3. **Незалежність:** підкидання монети вважається некорельованим без пам'яті або без хронології – що б не сталося перед процесом підкидання монети, це не вплине на процес.

Генератори випадкових бітів, вказані в цьому стандарті, намагаються імітувати серії підкидань монети, що ідеалізуються.

Непередбачуваність є необхідною властивістю генератора випадкових бітів (ГВБ). Якщо генератор випадкових бітів правильно реалізований і правильно працює, то неможливо передбачити вихідні дані. Неможливість пророцтва майбутніх вихідних даних (при відомих усіх попередніх випадкових бітах) визначається як **пряма секретність**. Неможливість визначення попередніх вихідних даних ГВБ при відомих існуючих або будь-яких майбутніх вихідних даних ГВБ визначається як **зворотна секретність**.

Обов'язковою вимогою при проектуванні НГВБ є наявність джерела (або джерел) ентропії (entropy source – ES) у вигляді фізичного генератора шуму. З урахуванням кінцевої надійності (тобто імовірність безвідмовної роботи менш одиниці) аналогових фізичних генераторів шуму (джерел ентропії) в стандарті ISO/IEC 18031:2005 введена вимога продовження роботи недетермінованого генератора випадкових бітів (НГВБ) способом, не менш захищеним, ніж детермінований генератор випадкових бітів (ДГВБ), у разі повного збою джерела (або усіх джерел) ентропії.

Стандарт ISO/IEC 18031:2005 не накладає жорсткі обмеження на параметри джерела ентропії. Це джерело може бути зміщеним (тобто імовірність появи нулів і одиниць на виході не обов'язково має бути рівною) і вихідні біти можуть навіть залежати один від одного. Єдина обов'язкова вимога – **джерело ентропії повинне генерувати біти з ненульовою ентропією**.

У обчислювальній техніці джерела ентропії найчастіше реалізують на основі генераторів шуму на кремнієвих діодах із Зенерівським пробоєм (стабілітронах). Структурна схема джерела ентропії включає: генератор аналогового шуму на діоді із Зенерівським пробоєм (DZ), компаратор (Cmp) для перетворення аналогових сигналів в рівні логічних мікросхем і рахунковий тригер (ТС) (рисунок 1).

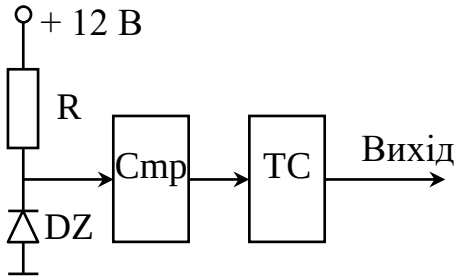

Рисунок 1 – Структура источника энтропии

Аналоговий сигнал на діоді із Зенерівським пробоєм (DZ) має вигляд коротких імпульсів з випадковими амплітудами, наступними один за одним через випадкові часові інтервали. Компаратор (Cmp) перетворює короткі вхідні імпульси в сигнали з нормованою амплітудою логічних мікросхем. Ці імпульси подаються на рахунковий тригер (СТ) для вирівнювання імовірності нульових і одиничних логічних рівнів (бітових сигналів) на виході джерела ентропії.

Значною мірою вимогам стандарту ISO/IEC 18031:2005 задовольняє генератор рівномірно розподілених випадкових бітових послідовностей, описаний в деклараційному патенті України [204]. Спрощена схема цього генератора наведена на рисунку 2.

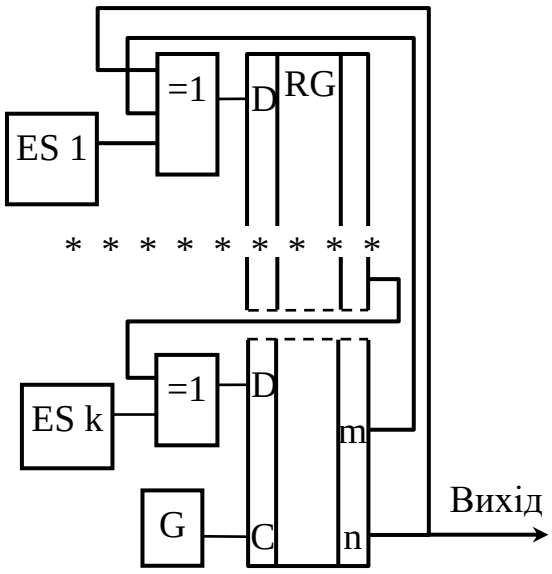

Рисунок 2 – Недетермінований
генератор випадкових бітів

Основу генератора складає лінійний рекурентний регістр (ЛРР), реалізований на регістрі зсуву (RG). На інформаційний вхід (D) цього регістра зсуву подається сигнал з виходу першого елементу «ВИКЛЮЧНЕ АБО» (елементу «XOR»), а до входів цього елементу підключені: останній вихід регістра зсуву «*n*» і проміжний вихід цього регістра «*m*».

Швидкість формування випадкових бітів визначається частотою тактового генератора (G).

Для того, щоб біти, які генеруються, були насправді випадковими (непередбачуваними, недетермінованими) до додаткового входу першого елементу «XOR» підключено перше джерело ентропії (entropy source – ES 1).

Перший елемент «ВИКЛЮЧНЕ АБО» передає сигнал зворотного зв'язку на вхід D регістра RG з інверсією (при одиничному сигналі на виході джерела ентропії) або без інверсії (при нульовому вихідному сигналі джерела ентропії). Таким чином, у випадкові моменти часу порушується порядок пересування нульових і одиничних бітів, який визначається параметрами рекуренти ЛРР. Вихідна випадкова бітова послідовність, яку можливо знімати з будь-якого виходу регістра зсуву, – стає непередбачуваною.

Для підвищення надійності в генератор випадкових бітових послідовностей введені декілька джерел ентропії (див. рисунок 1). Для цього регістр зсуву RG розбитий на *k* частин (необов'язково рівних) і на входи кожної частини регістра зсуву подаються сигнали з виходів попередніх частин цього регістра через елементи «ВИКЛЮЧНЕ АБО». Другі входи елементів «XOR» підключені до виходів додаткових джерел ентропії (ES 2…ES k).

Таке рішення дозволяє реалізувати «гаряче резервування» джерел ентропії ES, тобто їх паралельну роботу. Вихідні біти НГВБ залишаються випадковими (непередбачуваними) при справній роботі хоч би одного джерела ентропії (на виходах інших несправних джерел може бути «логічний нуль» або «логічна одиниця», тобто ентропія несправних джерел дорівнює нулю). Імовірність одночасного збою усіх джерел ентропії в цій схемі дуже мала і дорівнює добутку імовірностей збою кожного окремого джерела ентропії.

У разі повного збою усіх джерел ентропії такий генератор продовжує працювати як лінійний рекурентний регістр (ЛРР), тобто детермінований генератор псевдовипадкових послідовностей.

Відомі математичні алгоритми (наприклад, алгоритм Берлекемпа-Месі) дозволяють розрахувати основні параметри рекуренти ЛРР – «*m*» і «*n*» за результатами спостереження вихідної бітової послідовності, тривалість якої в 2 рази перевищує розрядність регістра зсуву «*n*». Тому криптостійкість такого генератора (тобто стійкість проти хакерських атак) при повному збої усіх джерел ентропії є недостатньою.

Існує декілька методів проектування детермінованих генераторів випадкових бітів, які руйнують лінійні властивості ЛРР і тим самим роблять такі системи криптографічний стійкішими:

- використання нелінійної функції, що об'єднує виходи декількох ЛРР (генератор Геффа та ін.);
- використання виходу одного ЛРР для управління синхросигналами іншого (чи декількох) ЛРР (алгоритм А5 та ін.);

- динамічна зміна параметрів рекуренти (довжини регістра «*n*» і номерів відводів «*m*») в процесі формування випадкових бітів, – так звані динамічні лінійні рекурентні регістри (ДЛРР).

Таке технічне рішення запропоноване в патенті [205]. На малюнку 3 наведена спрощена структурна схема цього пристрою.

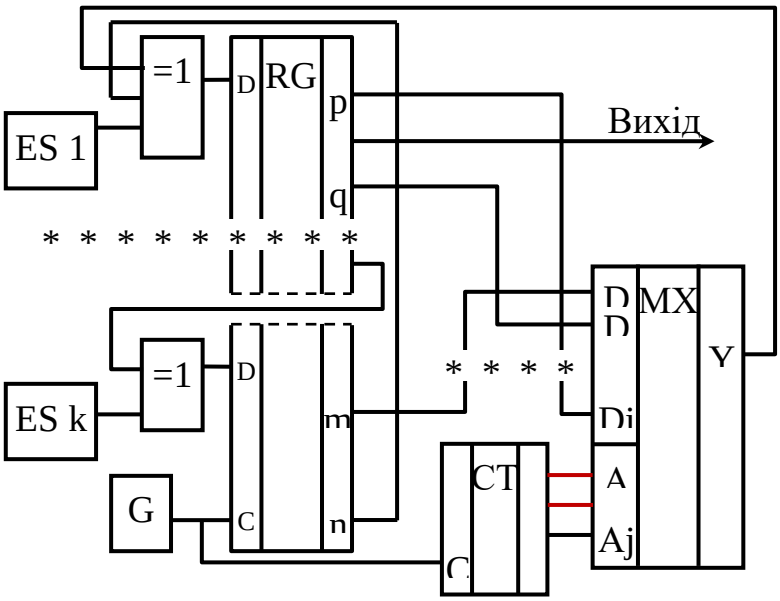

Рисунок 3 – Недетермінований генератор

випадкових бітів зі зміною параметрів рекуренти

На інформаційні входи (D1...Di) мультиплексора (MX) подаються сигнали з відводів регістра зсуву ЛЛР (RG). Номери усіх відводів повинні задовольняти відомій умові для ЛЛР [203]: поліном, який обчислюється на коефіцієнтах : $1 + x^m + x^n$ – має бути примітивним і неприведеним над полем Галуа.

Наприклад, для регістра зсуву (RG) з кількістю розрядів $n = 71$ цій умові задовольняють номери відводів ($p, q \ldots m$) : 6, 9, 18, 20, 35, 36, 51, 53, 62, 65 [203]. Для такого регістра зсуву з кількістю розрядів $n = 71$ і частоті формування псевдовипадкових бітів 10 ÷ 20 Мгц період повторення буде більше мільйона років, тобто періодичність такого ЛРР – практично нескінченна.

На адресні входи мультиплексора (A1…Aj) подаються вихідні сигнали старших розрядів двійкового лічильника (СТ). Кількість молодших розрядів

лічильника визначає інтервал часу між змінами параметрів рекуренти. Зазвичай цей інтервал менше часу генерації 2*n* вихідних випадкових бітів ($t_{2n} = 2n / F_G$, де: F_G – частота синхрогенератора G) в 5…10 разів. Така умова дозволяє за час генерації 2*n* вихідних випадкових бітів кілька разів поміняти параметр «*m*» рекуренти ЛРР. Це робить безглуздим застосування алгоритму Берлекемпа-Мессі для розрахунку параметра рекуренти ЛРР.

Кількість адресних входів мультиплексора (A1…Aj) дорівнює двійковому логарифму від кількості інформаційних входів (D1...Di).

Технічне рішення, запропоноване в патенті [206], дозволяє робити зміну параметрів рекурренти у випадковому порядку. На рисунку 4 наведена структурна схема цього НГВБ.

На адресні входи мультиплексора подаються випадкові коди з виходів паралельного регістра RG2, який запам'ятовує коди з довільних виходів регістра зсуву ЛРР (RG1).

Періодичність зміни кодів в паралельному регістрі RG2 визначається вихідним сигналом дільника з коефіцієнтом ділення, що програмується, (ДПКД) – СТ (рисунок 4). Коефіцієнт ділення визначається випадковими кодами, які знімаються з довільних виходів регістра зсуву ЛРР (RG1).

Для поліпшення статистичних властивостей вихідної випадкової бітової послідовності (конкретно: рівноймовірності і автокореляційної функції) декілька виходів ЛРР об'єднуються елементом «ВИКЛЮЧНЕ АБО» [203]. Вихід цього елементу є виходом недетермінованого генератора випадкових бітів.

У простішому варіанті (дивися патент [207]) інтервал часу для зміни кодів в паралельному регістрі RG2 задається лічильником СТ з постійним коефіцієнтом ділення. Цей коефіцієнт ділення має бути у декілька разів менше, ніж подвоєна розрядність регістра ЛЛР – 2*n*.

Кожен з цих недетермінованих генераторів випадкових бітів реалізований на одній логічній інтегральній схемі, що програмується, (ПЛІС) з кількістю тригерних комірок не менше 256.

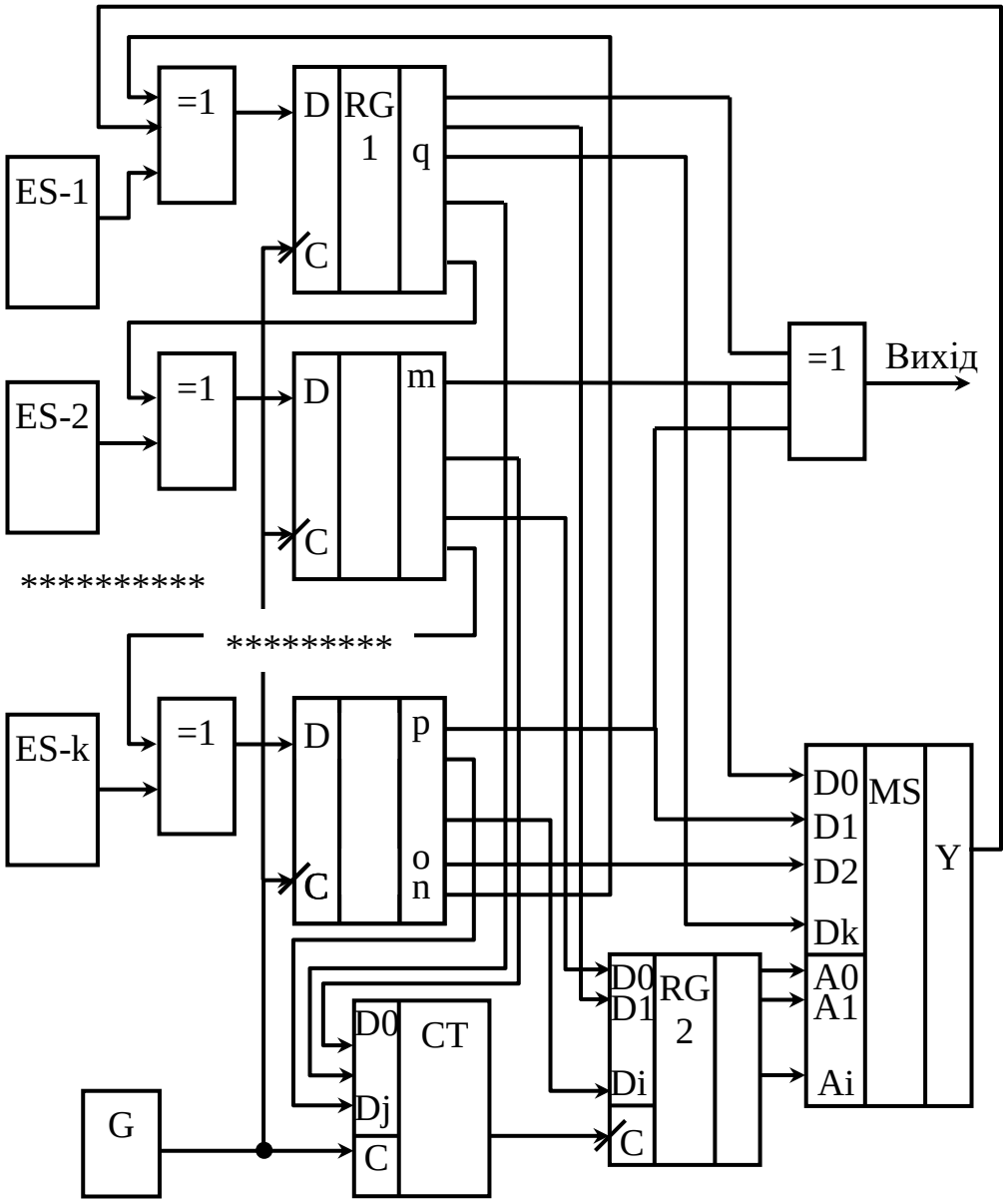

Рисунок 4 – Недетермінований генератор випадкових бітів зі зміною параметрів рекуренти у випадковому порядку

Аналогові складові джерел ентропії (діоди Зенера і компаратори) реалізовані на окремих елементах.

Усередині ПЛІС реалізовані також схеми контролю справності кожного джерела ентропії. При несправності усіх джерел ентропії робота НГВБ блокується і видається окремий сигнал «помилка».

Максимальна частота формування вихідних випадкових бітів визначається максимальною частотою роботи ПЛІС. Для сучасних ПЛІС ця частота може досягати десятків або сотень МГц.

Вихідні випадкові бітові послідовності кожного НГВБ проходили технологічне тестування [203]. Вибірка випадкової бітової послідовності завдовжки 8 Мбіт тестувалася п'ятьма тестами:

- монобітний тест (тест на рівноймовірність випадкових бітів),
- тест Покеру (тест на рівномірність появи блоків по 8 біт),
- автокореляційний тест і
- тест серій (тести на незалежність),
- тест довжини серій.

Час технологічного тестування на сучасних комп'ютерах не перевищує 1 сек.

Одноразове непопадання результатів одного з тестів в задані довірчі інтервали не може кваліфікуватися як непроходження тесту, тому що довірча імовірність події – попадання результатів тестування в довірчий інтервал – завжди менше одиниці (зазвичай обирається в діапазоні 0,95…0,99) [203].

Тільки при регулярному багатократному непопаданні результатів тестування в задані довірчі інтервали можливо стверджувати про невідповідність параметрів НГВБ моделі ідеального генератора випадкових бітів [203].

Усі запропоновані реалізації НГВБ підтверджували відповідність параметрів кожного НГВБ моделі ідеального генератора випадкових бітів.

Вихідні випадкові бітові послідовності кожного НГВБ проходили також повне тестування відповідно до рекомендацій NIST SP 800-22 (NIST STS) [203, 208]. Набір тестів NIST STS був запропонований в ході проведення конкурсу на новий національний стандарт США блокового шифрування. Цей набір застосовувався для досліджень статистичних властивостей кандидатів на новий блоковий шифр. На сьогодні методика тестування, яка запропонована NIST, є

найбільш поширеною у розробників криптографічних засобів захисту інформації.

Вибірка випадкової бітової послідовності на виході НГВБ завдовжки 100 Мбіт тестується 16 тестами. Час повного тестування відповідно до рекомендацій NIST SP 800-22 (NIST STS) на сучасних комп'ютерах складає 5…15 хв.

Усі запропоновані реалізації НГВБ підтверджували відповідність параметрів кожного НГВБ моделі ідеального генератора випадкових бітів за результатами тестування відповідно до рекомендацій NIST SP 800-22 (NIST STS).

В результаті розробки генераторів випадкових бітових послідовностей для криптографічних застосувань було встановлено, що недетермінований генератор випадкових бітів (НГВБ) відповідно до міжнародного стандарту ISO/IEC 18031:2005 обов'язково включає один або декілька джерел ентропії (ES) і детермінований механізм (алгоритм) криптографічного перетворення сигналів з виходів джерел ентропії у вихідні випадкові біти.

Це необхідно для виконання вимоги стандарту ISO/IEC 18031:2005 – продовження роботи недетермінованого генератора випадкових бітів (НГВБ) способом, не менш захищеним, ніж детермінований генератор випадкових бітів (ДГВБ), у разі повного збою джерела (або усіх джерел) ентропії. Для зменшення імовірності одночасного збою усіх джерел ентропії необхідно застосовувати гаряче резервування декількох джерел ентропії.

Наведені технічні рішення недетермінованих генераторів випадкових бітових послідовностей задовольняють вимогам стандарту ISO/IEC 18031:2005 і захищені патентами України.