УКРАЇНА

(19) UA (11) 97550 (13) C2

(51) МПК
G06F 7/58 (2006.01)
H03K 3/84 (2006.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

ОПИС
ДО ПАТЕНТУ НА ВИНАХІД

(54) НЕДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

(21) a201005237
(22) 29.04.2010
(24) 27.02.2012
(46) 27.02.2012, Бюл.№ 4, 2012 р.
(72) ТОРБА АЛЄКСАНДР АЛЄКСЄЄВІЧ, ГОРБЕНКО ІВАН ДМИТРОВИЧ, БОБУХ ВСЕВОЛОД АНАТОЛІЙОВИЧ, ТОРБА ГАННА ОЛЕКСАНДРІВНА, ЄЛАКОВ СЕРГІЙ ГЕННАДІЙОВИЧ
(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
(56) UA 50386 A; 15.10.2002
UA 82252 C2; 25.03.2008
UA 72655 C2; 15.03.2005
US 2010205235 A1; 12.08.2010
RU 2191421 C1; 20.10.2002
RU 2042187 C1; 20.08.1995
JP 3034516 B1; 17.04.2000
JP 2000298577 A; 24.10.2000
(57) Недетермінований генератор рівномірно розподілених випадкових послідовностей, що містить генератори випадкових логічних рівнів, перший канал рекурентного регістра зсуву, який складається з n_i елементів "ВИКЛЮЧНЕ АБО", перші входи яких підключені до виходів відповідних генераторів випадкових логічних рівнів, а виходи елементів "ВИКЛЮЧНЕ АБО" з'єднані з входами регістра зсуву, поділеного на n_i частин, а останні виходи кожної частини рекурентного регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", входи першого елемента "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом рекурентного регістра зсуву та проміжним виходом цього регістра, а також вихідний паралельний регістр, виходи якого підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами рекурентного регістра зсуву і входом лічильника імпульсів, а вихід цього лічильника під'єднаний до синхровходу вихідного паралельного регістра та входу тригера "прапора", вихід якого з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент "І" з шиною даних ПЕОМ, і дешифратор адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного паралельного регістра і входу скидання тригера "прапора", і другим виходом до буферного елемента "І", який **відрізняється** тим, що додатково введені $i\text{-}n_1$ генераторів випадкових логічних рівнів, k-1 каналів рекурентних регістрів зсуву, причому кожен канал складається з регістра зсуву, поділеного на n_k частин, і додаткових n_k елементів "ВИКЛЮЧНЕ АБО", з'єднаних аналогічно першому каналу, а також m елементів "ВИКЛЮЧНЕ АБО", виходи яких підключені до входів вихідного паралельного регістра, а входи цих елементів "ВИКЛЮЧНЕ АБО" з'єднані з виходами рекурентних регістрів зсуву від усіх каналів у довільному порядку.

(19) UA (11) 97550 (13) C2

Винахід належить до області обчислювальної техніки і може бути використаний в системах захисту інформації обчислювальних систем, наприклад, при генерації параметрів алгоритмів криптографічного перетворення, в протоколах аутентифікації, в засобах імовірнісного кодування та ін.

Відомий генератор випадкових чисел [див. рис. 4 в статті: Торба А.А., Елаков С.Г., Степченко А.З. Генерация равновероятных случайных последовательностей на основе физических датчиков // Радиотехника. Всеукр. міжвід. наук.-техн. зб. 2001. Вип. 119, с. 108-113.], що містить вузол генерації випадкових логічних рівнів, який складається з послідовно з'єднаних генератора шуму (фізичного датчика шуму), підсилювача-обмежувача та лічильного тригера, вихід якого з'єднано з входом дворозрядного регістра зсуву, виходи якого увімкнуті до входів елемента "ВИКЛЮЧНЕ АБО", а вихід цього елемента з'єднано з

входом даних вихідного регістра зсуву, виходи якого є виходами генератора випадкових чисел, тактовий генератор, вихід якого з'єднаний з синхровходом дворозрядного регістра зсуву і входом дільника на 2, вихід якого з'єднано з синхровходом вихідного регістра зсуву.

Недоліком цього генератора є невелика швидкість формування випадкових бітів в порівнянні з частотою шумових імпульсів фізичного датчика, тому що підвищення частоти тактового генератора призводить до того, що імовірності формування випадкових одиниць або нулів не тільки не вирівнюються, а навпаки, ще більше розрізняються за рахунок статистичного зв'язку між логічними рівнями на входах елемента "ВИКЛЮЧНЕ АБО".

Недоліком цього генератора також є невідповідність спеціальним вимогам стандарту ISO/IEC 18031:2005, яких необхідно дотримуватися при розробці генератора випадкових бітів, що буде використовуватися для криптографічних застосувань. Цей генератор не підтримує "вимогу продовження дії недетермінованого генератора випадкових бітів (НГВБ) способом, не менш захищеним, ніж детермінований генератор випадкових бітів (ДГВБ) у випадку повного збою джерела ентропії".

Найбільш близьким по сукупності ознак є генератор рівномірно розподілених випадкових послідовностей [див. патент України № 50386 А, МПК6 G06F7/58, G07C15/00, опублікований 15.10.2002, Бюл. № 1], що містить n генераторів випадкових логічних рівнів, які складаються з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, виходи генераторів випадкових логічних рівнів підключені до перших входів n елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра зсуву, поділеного на n частин, а останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", входи першого елемента "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом регістра зсуву та проміжним виходом цього регістра, виходи регістра зсуву підключені до входів вихідного паралельного регістра, а його виходи підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входом лічильника імпульсів, вихід якого під'єднаний до синхровходу вихідного паралельного регістра та входу тригера "прапора", а його вихід з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент "І" з шиною даних ПЕОМ, та дешифратор адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного регістра і входу скидання тригера "прапора", і другим виходом до буферного елемента "І".

Недоліком цього генератора є його недостатня надійність та криптостійкість у випадку повного збою генераторів випадкових логічних рівнів або у випадку непрацездатності одного з тригерів регістра зсуву.

В основу винаходу поставлена задача створення такого недетермінованого генератора рівномірно розподілених випадкових послідовностей, в якому додавання нових схемних елементів і зв'язків дозволило б підвищити надійність та криптостійкість за рахунок паралельної роботи декількох каналів з рекурентними регістрами зсуву та формування усіх вихідних випадкових бітів об'єднанням елементами "ВИКЛЮЧНЕ АБО" випадкових бітів з виходів рекурентних регістрів зсуву від усіх каналів.

Такий технічний результат може бути досягнутий, якщо в недетермінованому генераторі рівномірно розподілених випадкових послідовностей, що містить n_1 генераторів випадкових логічних рівнів, перший канал рекурентного регістра зсуву, який складається з n_1 елементів "ВИКЛЮЧНЕ АБО", перші входи яких підключені до виходів генераторів випадкових логічних рівнів, а виходи елементів "ВИКЛЮЧНЕ АБО" з'єднані з входами регістра зсуву, поділеного на n_1 частин, а останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", входи першого елемента "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом регістра зсуву та проміжним виходом цього регістра, а також вихідний паралельний регістр, виходи якого підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами рекурентного регістра зсуву і входом лічильника імпульсів, а вихід цього лічильника під'єднаний до синхровходу вихідного паралельного регістра та входу тригера "прапора", вихід якого з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент "І" з шиною даних ПЕОМ, і дешифратор адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного паралельного регістра і входу скидання тригера "прапора", і другим виходом до буферного елемента "І", згідно з винаходом, додатково введені $i\text{-}n_1$ генераторів випадкових логічних рівнів, k-1 канали рекурентних регістрів зсуву, причому кожен канал складається з регістра зсуву, поділеного на n_k частин, і додаткових n_k елементів "ВИКЛЮЧНЕ АБО", з'єднаних аналогічно першому каналу, а також m елементів "ВИКЛЮЧНЕ АБО", виходи яких підключені до входів вихідного паралельного регістра, а входи цих елементів "ВИКЛЮЧНЕ АБО" з'єднані з виходами рекурентних регістрів зсуву від усіх каналів у довільному порядку.

Таким чином, введення в недетермінований генератор рівномірно розподілених випадкових послідовностей додаткових $i\text{-}n_1$ генераторів випадкових логічних рівнів та k-1 каналів рекурентних регістрів зсуву, які складаються з елементів "ВИКЛЮЧНЕ АБО" і регістрів зсуву, а також з'єднання у довільному порядку логічних сигналів з виходів рекурентних регістрів зсуву від усіх каналів додатковими елементами "ВИКЛЮЧНЕ АБО" дозволяє підвищити надійність пристрою за рахунок гарячого резервування каналів рекурентних регістрів зсуву, а також у випадку повної працездатності усіх каналів еквівалентна довжина рекурентного регістра зсуву дорівнює сумі довжин усіх каналів, такий засіб підвищує криптостійкість випадкових послідовностей, що генеруються.

На фігурі зображена структурна схема недетермінованого генератора рівномірно розподілених випадкових послідовностей.

На фігурі використані наступні міжнародні позначення: ES - генератори випадкових логічних рівнів, RG - регістр, G - генератор, CT - лічильник, T - тригер, DC - дешифратор.

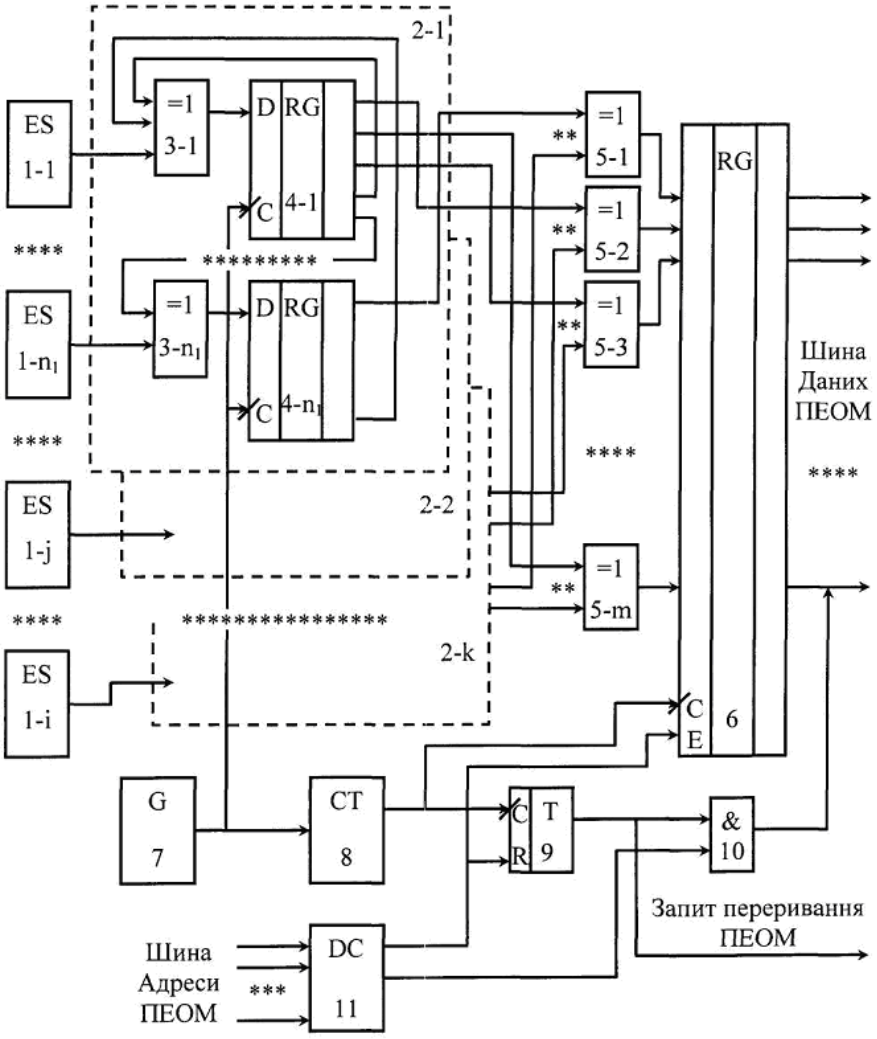
Недетермінований генератор рівномірно розподілених випадкових послідовностей містить і джерел 1-1…1-і ентропії, які підключені до каналів 2-1…2-k рекурентних регістрів зсуву, при чому кожен канал 2-1…2-k складається з елементів 3-1…3-n_k "ВИКЛЮЧНЕ АБО" і регістра 4-1…4-n_k зсуву, поділеного на n_k частин, в кожному каналі 2-1…2-k рекурентних регістрів зсуву перші входи елементів 3-1…3-n_k "ВИКЛЮЧНЕ АБО" підключені до виходів генераторів випадкових логічних рівнів 1-1…1-n_k, а виходи елементів 3-1…3-n_k "ВИКЛЮЧНЕ АБО" з'єднані з входами регістра 4-1…4-n_k зсуву, поділеного на $n_к$ частин, а останні виходи кожної частини регістра 4-1…4-n_k зсуву підключені до других входів наступних елементів 3-1…3-n_k "ВИКЛЮЧНЕ АБО", входи першого елемента 3-1 "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом регістра 4-n_k зсуву та проміжним виходом цього регістра 4-1…4-n_k, а також вихідний паралельний регістр 6, виходи якого підключені до шини даних ПЕОМ, а входи вихідного паралельного регістра 6 з'єднані з виходами m елементів 5-1…5-m "ВИКЛЮЧНЕ АБО", входи яких підключені у довільному порядку до виходів рекурентних регістрів 4-1…4-n_k зсуву від кожного каналу 2-1…2-k, тактовий генератор 7, вихід якого з'єднаний з синхровходами регістрів 4-1…4-n_k зсуву усіх каналів 2-1…2-k а також з входом лічильника 8 імпульсів, а його вихід під'єднаний до синхровходу вихідного паралельного регістра 6 та входу тригера 9 "прапора", а вихід тригера 9 "прапора" з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент 10 "І" з шиною даних ПЕОМ, дешифратор 11 адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного паралельного регістра 6 і входу скидання тригера 9 "прапора", і другим виходом до буферного елемента 10 "І".

Недетермінований генератор рівномірно розподілених випадкових послідовностей працює наступним чином.

На виходах генераторів випадкових логічних рівнів 1-1…1-і формуються логічні рівні, які з рівною імовірністю приймають значення нуля або одиниці в випадкові моменти часу. Ці випадкові логічні рівні перемикають на протилежні значення логічні рівні, що подаються з останніх виходів частин регістрів 4-1…4-n_k зсуву до входів наступних частин цих регістрів, в випадкові моменти часу за допомогою елементів 3-1…3-n_k "ВИКЛЮЧНЕ АБО". Тактовий генератор 7 визначає частоту зсуву випадкових бітів в рекурентних регістрах 4-1…4-n_k і таким чином визначає швидкість формування випадкових послідовностей, які за рахунок дії генераторів випадкових логічних рівнів 1-1…1-і стають непередбачуваними, тобто - недетермінованими, непрогнозованими.

Лічильник 8 імпульсів через задане число періодів тактового генератора 7 формує імпульс для запису коду з виходів елементів 5-1…5-m "ВИКЛЮЧНЕ АБО" у вихідний паралельний регістр 6 та для установи тригера 9 "прапора" в одиничний стан. Кількість елементів 5-1…5-m "ВИКЛЮЧНЕ АБО" дорівнює кількості розрядів m вихідного паралельного регістра 6. Входи усіх елементів 5-1…5-m "ВИКЛЮЧНЕ АБО" з'єднані у довільному порядку з виходами рекурентних регістрів 4-1…4-n_k зсуву від усіх каналів 2-1…2-k.

Вихідний сигнал тригера 9 "прапора" подається на вхід запиту переривання ПЕОМ. Виконуючи підпрограму обробки переривання, ПЕОМ зчитує випадкову послідовність довжиною m бітів з вихідного паралельного регістра 6 на шину даних. Для цього на шину адреси ПЕОМ виставляється адреса порту пристрою, що розпізнається дешифратором 11 адреси. Вихідний сигнал дешифратора 11 дозволяє зчитування коду вихідного паралельного регістра 6, а також скидає у нуль тригер 9 "прапора". Стан тригера 9 "прапора" може бути також прочитаний на шині даних ПЕОМ через буферний елемент 10 "І", на вхід якого подається імпульс з другого виходу дешифратора 11 адреси.



Комп'ютерна верстка Г. Паяльніков

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601