УКРАЇНА

(19) UA (11) 70165 (13) U

(51) МПК (2012.01)
G06F 7/00
G07C 15/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2011 14446**

(22) Дата подання заявки: **06.12.2011**

(24) Дата, з якої є чинними права на корисну модель: **25.05.2012**

(46) Публікація відомостей про видачу патенту: **25.05.2012, Бюл.№ 10**

(72) Винахідник(и):
Торба Алєксандр Алєксєєвіч (UA),
Бобух Всеволод Анатолійович (UA),
Бобкова Анна Алєксандровна (UA),
Торба Олег Олександрович (UA),
Торба Дмитро Олександрович (UA),
Єлаков Сергій Геннадійович (UA)

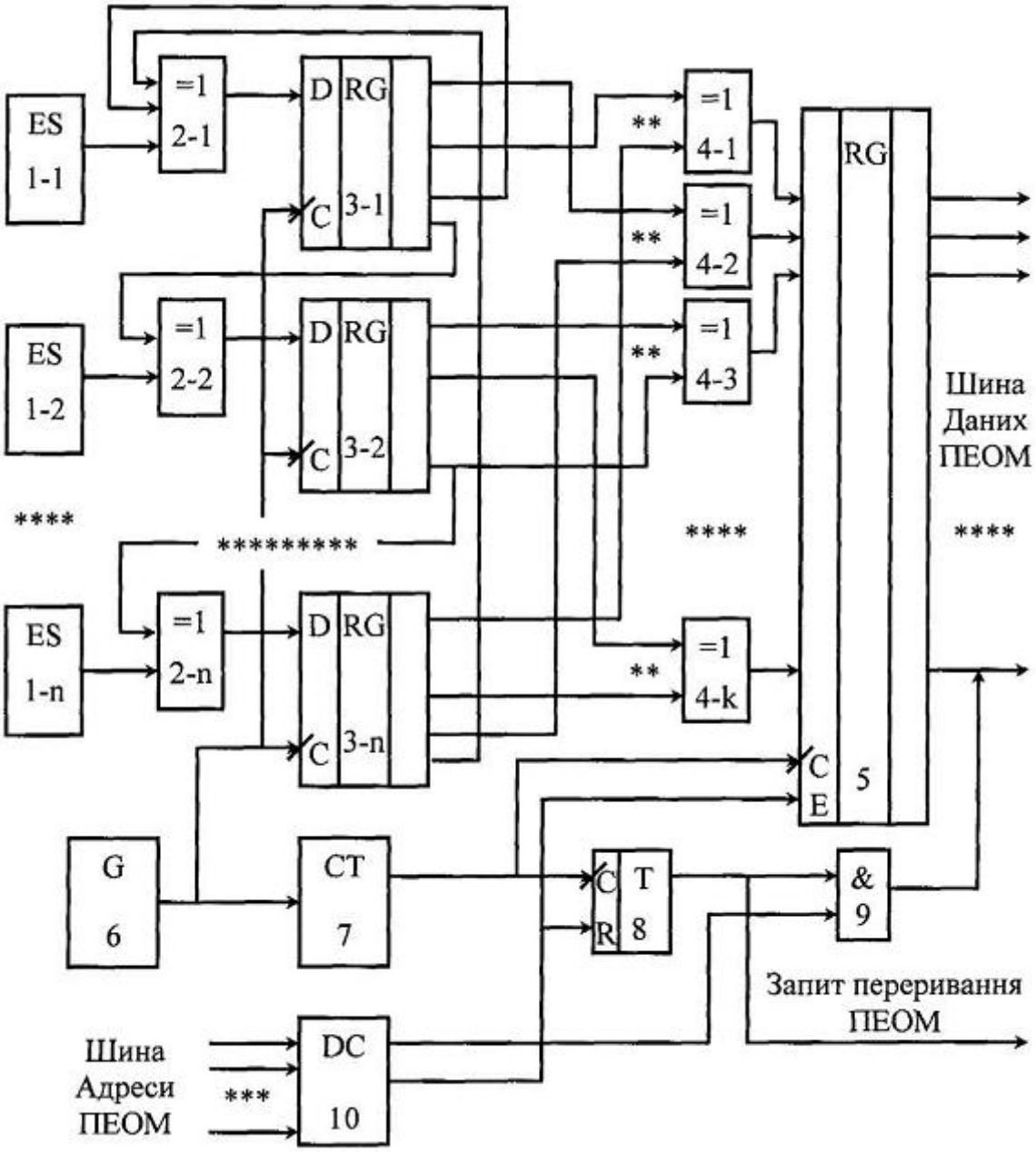
(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Леніна, 14, м. Харків, 61166 (UA)

(54) НЕДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

(57) Реферат:

Недетермінований генератор рівномірно розподілених випадкових послідовностей містить n джерел ентропії, підключених 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". Додатково введені k елементів "ВИКЛЮЧНЕ АБО", виходи яких підключені до входів вихідного паралельного регістра, а входи цих елементів з'єднані з виходами регістра зсуву у довільному порядку. Коефіцієнт ділення лічильника імпульсів повинен бути більший кількості розрядів вихідного паралельного регістра.

UA 70165 U


ES
1-1
=1
2-1
D RG
C 3-1
ES
1-2
=1
2-2
D RG
C 3-2
ES
1-n
=1
2-n
D RG
C 3-n
**
=1
4-1
=1
4-2
=1
4-3
=1
4-k
RG
C
E
5
Шина
Даних
ПЕОМ
****
****
G
6
CT
7
C T
R 8
&
9
Запит переривання
ПЕОМ
Шина
Адреси
ПЕОМ
***
DC
10

Фіг.

Корисна модель належить до галузі обчислювальної техніки і може бути використана 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. між-від. 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 схеми "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 схеми "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. № 10), що містить n джерел ентропії, які складаються з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, виходи джерел ентропії 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 елементу "І".

Недоліком цього генератора є його недостатня криптостійкість у випадку повного збою джерел ентропії.

В основу корисної моделі поставлена задача створення такого недетермінованого генератора рівномірно розподілених випадкових послідовностей, в якому додавання нових схемних елементів і зв'язків дозволило б підвищити криптостійкість за рахунок формування усіх вихідних випадкових бітів об'єднанням елементами "ВИКЛЮЧНЕ АБО" випадкових бітів з виходів регістра зсуву.

Такий технічний результат може бути досягнутий, якщо в недетермінованому генераторі рівномірно розподілених випадкових послідовностей, що містить n джерел ентропії, підключених 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, вихідний паралельний регістр, виходи якого підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входом лічильника імпульсів, а його вихід 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 корисною моделлю, додатково введені k елементів "ВИКЛЮЧНЕ АБО", виходи яких підключені до входів вихідного паралельного регістра, а входи цих елементів з'єднані з виходами регістра зсуву у довільному порядку, та коефіцієнт ділення лічильника імпульсів повинен бути більший кількості розрядів вихідного паралельного регістра.

Таким чином, введення в недетермінований генератор рівномірно розподілених випадкових послідовностей додаткових k елементів "ВИКЛЮЧНЕ АБО", з'єднаних у довільному порядку з виходами регістра зсуву та збільшення коефіцієнта ділення лічильника імпульсів дозволяє довільно змінити порядок виводу випадкових бітів та значно ускладнити процес криптоаналізу цих послідовностей за рахунок неможливості дослідження безперервного потоку випадкових бітів.

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

На кресленні використані наступні міжнародні позначення: ES - джерело ентропії, RG - регістр, G - генератор, CT - лічильник, T - тригер, DC - дешифратор.

Недетермінований генератор рівномірно розподілених випадкових послідовностей містить n джерел 1-1…1-n ентропії, підключених до перших входів елементів 2-1…2-n "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра 3-1…3-n зсуву, поділеного на n частин, а останні виходи кожної частини регістра 3-1…3-n зсуву підключені до других входів наступних елементів 2-2…2-n "ВИКЛЮЧНЕ АБО", входи першого елемента 2-1 "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом регістра 3-n зсуву та проміжним виходом цього регістра 3-1…3-n, вихідний паралельний регістр 5, виходи якого підключені до шини даних ПЕОМ, а входи вихідного паралельного регістра 5 з'єднані з виходами k елементів 4-1…4-k "ВИКЛЮЧНЕ АБО", входи яких підключені у довільному порядку до виходів регістра 3-1…3-n зсуву, тактовий генератор 6, вихід якого з'єднаний з синхровходами регістра 3-1…3-n зсуву і входом лічильника 7 імпульсів, а його вихід під'єднаний до синхровходу вихідного паралельного регістра 5 та входу тригера 8 "прапора", а вихід тригера 8 "прапора" з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент 9 "І" з шиною даних ПЕОМ, і дешифратор 10 адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного паралельного регістра 5 і входу скидання тригера 8 "прапора", і другим виходом до буферного елемента 9 "І".

Недетермінований генератор рівномірно розподілених випадкових послідовностей працює наступним чином.

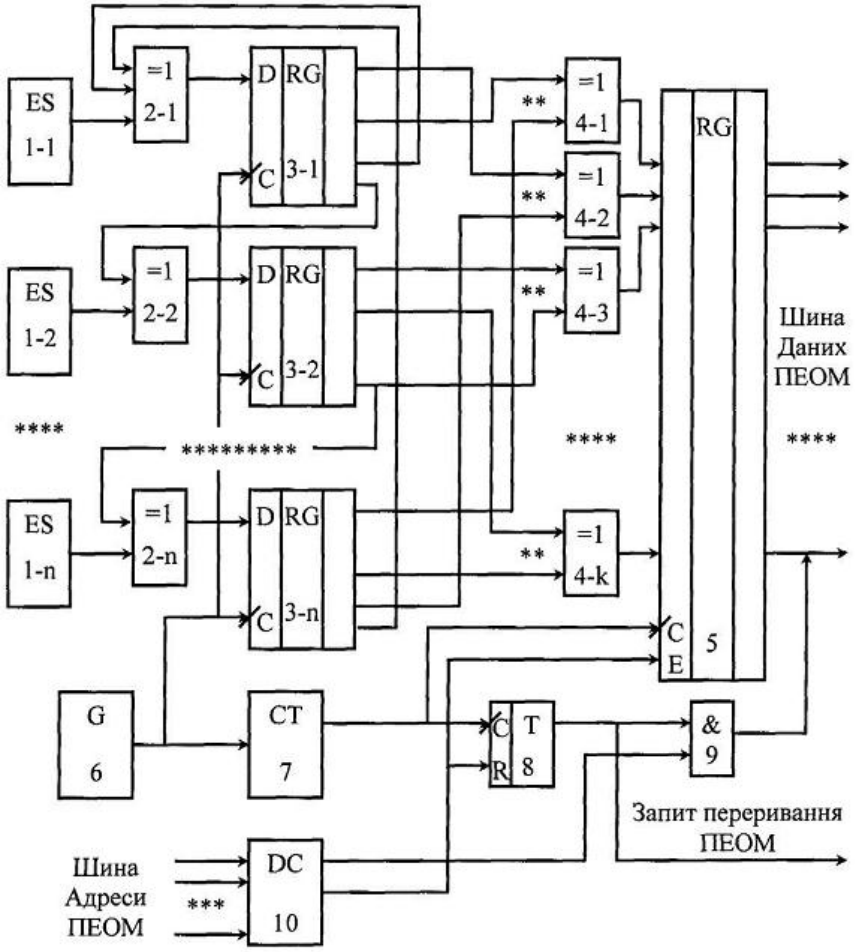
На виходах джерел 1-1…1-n ентропії формуються логічні рівні, які з рівною імовірністю приймають значення нуля або одиниці в випадкові моменти часу. Ці випадкові логічні рівні перемикають на протилежні значення логічні рівні, що подаються з останніх виходів частин регістра 3-1…3-n зсуву до входів наступних частин цього регістра, в випадкові моменти часу за допомогою елементів 2-1…2-n "ВИКЛЮЧНЕ АБО". Тактовий генератор 6 визначає частоту зсуву випадкових бітів в регістрі 3-1…3-n і таким чином визначає швидкість формування випадкових послідовностей, які за рахунок дії джерел 1-1…1-n ентропії стають непередбачуваними, тобто - недетермінованими, непрогнозованими.

Лічильник 7 імпульсів через задане число періодів тактового генератора 6 формує імпульс для запису коду з виходів елементів 4-1…4-k "ВИКЛЮЧНЕ АБО" у вихідний паралельний регістр 5 та для установи тригера 8 "прапора" в одиничний стан. Кількість елементів 4-1…4-k "ВИКЛЮЧНЕ АБО" дорівнює кількості розрядів k вихідного паралельного регістра 5. Входи усіх елементів 4-1…4-к "ВИКЛЮЧНЕ АБО" з'єднані у довільному порядку з виходами регістра 3-1…3-n зсуву. Вихідний сигнал тригера 8 "прапора" подається на вхід запиту переривання ПЕОМ. Виконуючи підпрограму обробки переривання, ПЕОМ зчитує випадкову послідовність довжиною k бітів з вихідного паралельного регістра 5 на шину даних. Для цього на шину адреси ПЕОМ виставляється адреса порту пристрою, що розпізнається дешифратором 10 адреси. Вихідний сигнал дешифратора 10 дозволяє зчитування коду вихідного паралельного регістра 5, а також скидає в нуль тригер 8 "прапора". Стан тригера 8 "прапора" може бути також прочитаний на шині даних ПЕОМ через буферний елемент 9 "І", на вхід якого подається імпульс з другого виходу дешифратора 10 адреси.

Коефіцієнт ділення лічильника 7 імпульсів повинен бути більший кількості розрядів k вихідного паралельного регістра 5. Це унеможливлює послідовне зчитування у ПЕОМ усіх випадкових бітів, що генеруються, і таким чином значно ускладнює процес критоаналізу цих окремих випадкових бітових послідовностей.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Недетермінований генератор рівномірно розподілених випадкових послідовностей, що містить n джерел ентропії, підключених 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, вихідний паралельний регістр, виходи якого підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входом лічильника імпульсів, а його вихід 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 k елементів "ВИКЛЮЧНЕ АБО", виходи яких підключені до входів вихідного паралельного регістра, а входи цих елементів з'єднані з виходами регістра зсуву у довільному порядку, та коефіцієнт ділення лічильника імпульсів повинен бути більший кількості розрядів вихідного паралельного регістра.



Комп'ютерна верстка Д. Шеверун

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