



УКРАЇНА

(19) **UA** (11) **99017** (13) **C2**
(51) МПК (2012.01)
G06F 7/00
G06C 15/00

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД

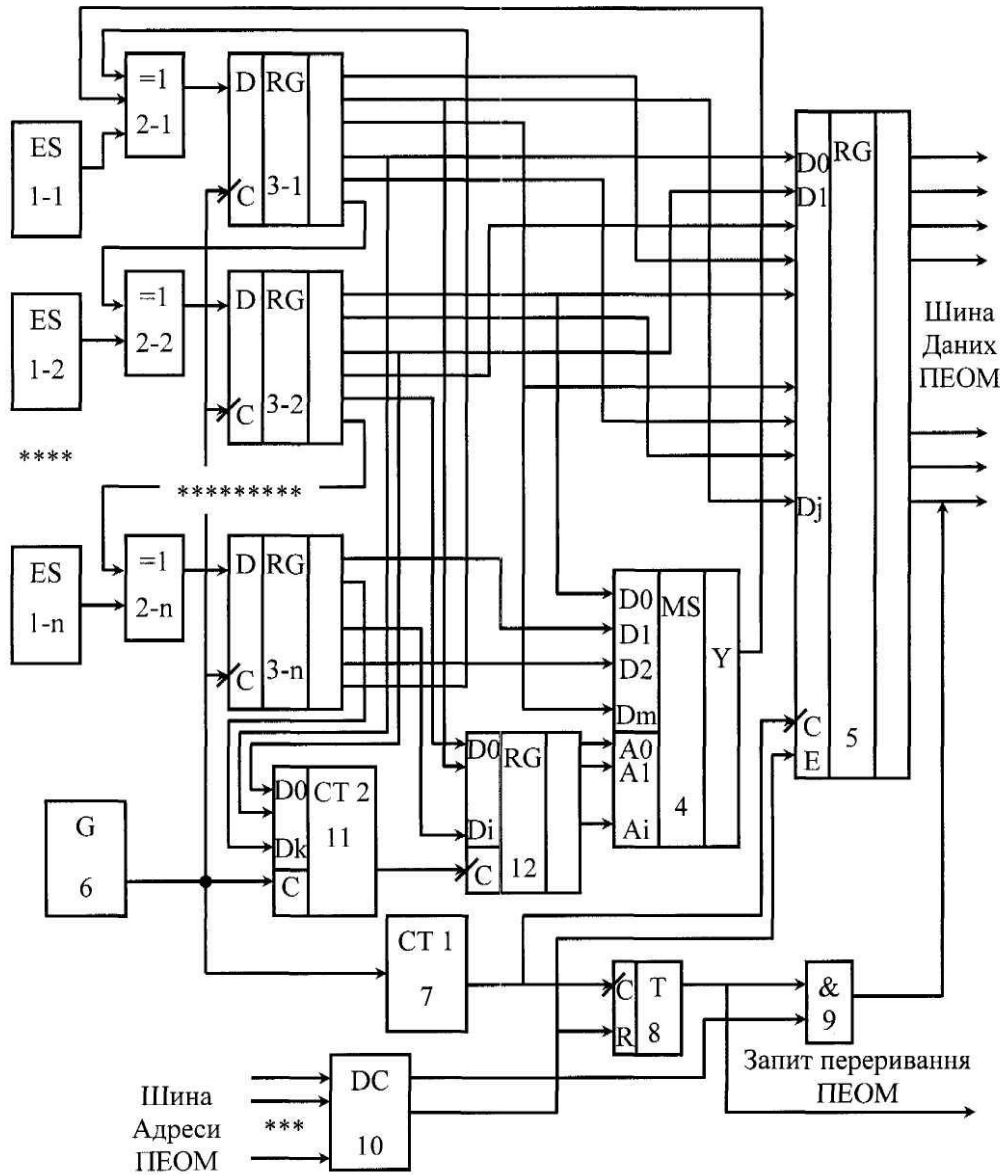
(21) Номер заявки: а 2010 13538	(72) Винахідник(и): Торба Александр Алексеевич (UA), Горбенко Іван Дмитрович (UA), Бобух Всеволод Анатолійович (UA), Бобкова Анна Александровна (UA), Слаков Сергій Геннадійович (UA)
(22) Дата подання заявки: 15.11.2010	
(24) Дата, з якої є чинними права на винахід: 10.07.2012	
(41) Публікація відомостей про заявку: 25.05.2012, Бюл.№ 10	(73) Власник(и): ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ, пр. Леніна, 14, м. Харків, 61166, Україна (UA)
(46) Публікація відомостей про видачу патенту: 10.07.2012, Бюл.№ 13	(56) Перелік документів, взятих до уваги експертизою: UA 52410 U; 25.08.2010 UA 50386 A; 15.10.2002 UA 82252 C2; 25.03.2008 UA 86979 C2; 10.06.2009 JP 2007179524 A; 12.07.2007 WO 2009063948 A1; 22.05.2009 US 2003219119 A1; 27.11.2003 JP 3034516 B1; 17.04.2000 JP 2000298577 A; 24.10.2000 WO 02071204 A1; 12.09.2002

(54) НЕДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

(57) Реферат:

Недетермінований генератор рівномірно розподілених випадкових послідовностей належить до обчислювальної техніки, а саме до системи захисту інформації обчислювальних систем. Генератор містить джерела ентропії, елементи "ВИКЛЮЧНЕ АБО", реєстри, мультиплексор, тактовий генератор, лічильники, тригер та дешифратор. При цьому другий лічильник імпульсів виконано як лічильник зі змінним коефіцієнтом ділення, а інформаційні входи цього лічильника підключені до проміжних виходів реєстра зсуву у довільному порядку. Технічним результатом є підвищення криптостійкості випадкових послідовностей, що генеруються.

UA 99017 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 рівномірно розподілених випадкових послідовностей (патент України №50386 А, МПК6 G06F 7/58, G07C 15/00, опублік. 15.10.2002, Бюл. №10), що містить п джерел ентропії, які складаються з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, виходи джерел ентропії підключені до перших входів п елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра зсуву, поділеного на п 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 можливість прорахунку послідовності вихідних псевдовипадкових бітів на підставі відомих математичних моделей у випадку повного збою джерел ентропії.

Найбільш близьким по сукупності ознак є генератор рівномірно розподілених випадкових послідовностей (патент України на корисну модель №52410, МПК(2009) G06F 7/00, G07C 15/00, опублік. 25.08.2010, Бюл. №16), що містить п джерел ентропії, які складаються з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, виходи джерел ентропії підключені до перших входів п елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра зсуву, поділеного на п 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 виходом мультиплексора, інформаційні входи якого під'єднані у довільному порядку до проміжних виходів регістра зсуву, а адресні входи мультиплексора підключені до виходів додаткового паралельного регістра, інформаційні входи цього регістра з'єднані з проміжними виходами регістра зсуву у довільному порядку, вхід синхронізації додаткового паралельного регістра підключений до виходу другого лічильника імпульсів, виходи регістра зсуву з'єднані у довільному порядку з входами вихідного паралельного регістра, а його виходи підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входами першого та другого лічильників імпульсів, вихід першого лічильника 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 криптостійкість у випадку повного збою джерел ентропії, тому що параметри рекуренти регістра зсуву змінюються з постійною періодичністю, яка визначається коефіцієнтом ділення другого лічильника імпульсів.

Технічною задачею винаходу є підвищення криптостійкості недетермінованого генератора рівномірно розподілених випадкових послідовностей за рахунок зміни параметрів рекуренти регістра зсуву у непередбачувані моменти часу, що забезпечується новими схемними елементами і зв'язками.

Такий технічний результат може бути досягнутий, якщо в недетермінованому генераторі рівномірно розподілених випадкових послідовностей, що містить п джерел ентропії, підключених до перших входів п елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра зсуву, поділеного на п 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 виходом мультиплексора, інформаційні входи якого під'єднані у довільному порядку до проміжних виходів регістра зсуву, а адресні входи мультиплексора підключені до виходів додаткового паралельного регістра, інформаційні входи цього регістра з'єднані з проміжними виходами регістра зсуву у довільному порядку, вхід синхронізації додаткового паралельного регістра підключений до виходу другого лічильника імпульсів, виходи регістра зсуву з'єднані у довільному порядку з входами вихідного

паралельного регістру, а його виходи підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входами першого та другого лічильників імпульсів, а вихід першого лічильника імпульсів під'єднаний до синхровходу вихідного паралельного регістра та входу тригера "прапора", вихід якого з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент "I" 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 "I", згідно з винаходом, другий лічильник імпульсів виконано як лічильник зі змінним коефіцієнтом ділення, а інформаційні входи цього лічильника підключені до проміжних виходів регістра зсуву у довільному порядку.

Таким чином, виконання другого лічильників імпульсів як лічильника зі змінним коефіцієнтом ділення та додавання нових зв'язків дозволяє змінювати параметри рекуренти регістра зсуву у непередбачувані моменти часу, які визначаються випадковими кодами, що подаються на інформаційні входи цього лічильника.

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

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

Генератор 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", другий вхід першого елемента 2-1 "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра 3-n зсуву, а третій вхід першого елемента 2-1 "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора 4, інформаційні входи якого підключені до проміжних виходів регістра 3-1...3-n зсуву, вихідний паралельний регістр 5, виходи якого підключені до шини даних ПЕОМ, а входи вихідного паралельного регістра 5 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 першого лічильника 7 імпульсів, вихід якого 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 "I" 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 "I", другий лічильник 11 імпульсів зі змінним коефіцієнтом ділення, синхровхід якого з'єднаний з виходом тактового генератора 6, а інформаційні входи другого лічильника 11 імпульсів підключені до проміжних виходів регістра 3-1...3-n зсуву у довільному порядку, вихід другого лічильника 11 імпульсів зі змінним коефіцієнтом ділення з'єднаний з синхровходом додаткового паралельного регістра 12, інформаційні входи якого підключені до проміжних виходів регістра 3-1...3-n зсуву, а виходи додаткового паралельного регістра підключені до адресних входів мультиплексора 4.

Генератор рівномірно розподілених випадкових послідовностей працює наступним чином.

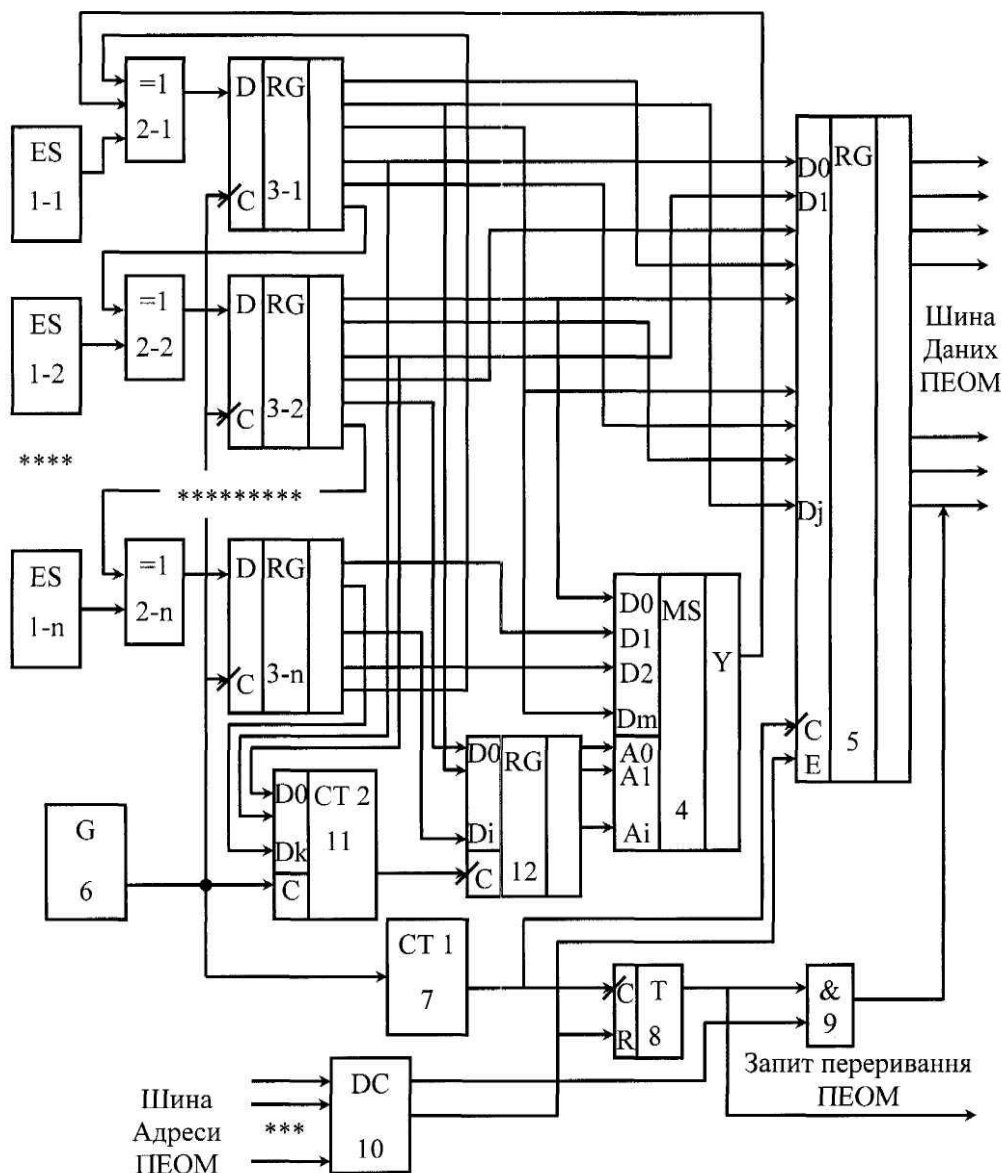
На виходах джерел 1-1...1-n ентропії формуються логічні рівні, які з рівною імовірністю приймають значення нуля або одиниці в випадкові моменти часу. Ці випадкові логічні рівні перемикають на протилежні значення логічні рівні, що подаються з останніх виходів частин регістра 3-1...3-n зсуву до входів 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 бітових послідовностей, які за рахунок дії джерел 1-1...1-n ентропії стають непередбачуваними, тобто - недетермінованими, непрогнозованими.

Перший лічильник 7 імпульсів через задане число періодів тактового генератора 6 формує імпульс для запису коду з регістра 3-1...3-n зсуву у довільному порядку у вихідний паралельний регістр 5 та для установи тригера 8 "прапора" одиничний стан. Вихідний сигнал тригера 8 "прапора" подається на вхід запиту переривання ПЕОМ. Виконуючи підпрограму обробки переривання, ПЕОМ зчитує випадкове число 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 "I", на вхід якого подається імпульс з другого виходу дешифратора 10 адреси.

Для зміни параметрів рекуренти регістра 3-1...3-п зсуву його логічні рівні з проміжних виходів подаються на інформаційні входи мультиплексора 4, вихід якого підключено до третього входу елемента 2-1 "ВИКЛЮЧНЕ АБО". Порядок зміни параметрів рекуренти визначається випадковими кодами, які подаються на адресні входи мультиплексора 4 з виходів додаткового паралельного регістра 12, інформаційні входи якого підключені до проміжних виходів регістра 3-1...3-п зсуву у довільному порядку, а синхровхід додаткового паралельного регістра 12 з'єднаний з виходом другого лічильника 11 імпульсів зі змінним коефіцієнтом ділення. Коефіцієнт ділення цього лічильника 11 імпульсів постійно змінюється за рахунок випадкових кодів, які подаються на його інформаційні входи, тому проміжки часу зміни параметрів рекуренти регістра 3-1...3-п зсуву також постійно змінюються та є непередбачуваними.

ФОРМУЛА ВИНАХОДУ

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 виходом мультиплексора, інформаційні входи якого під'єднані у довільному порядку до проміжних виходів регістра зсуву, а адресні входи мультиплексора підключені до виходів додаткового паралельного регістра, інформаційні входи цього регістра з'єднані з проміжними виходами регістра зсуву у довільному порядку, вхід синхронізації додаткового паралельного регістра підключений до виходу другого лічильника імпульсів, виходи регістра зсуву з'єднані у довільному порядку з входами вихідного паралельного регістра, а його виходи підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входами першого та другого лічильників імпульсів, а вихід першого лічильника імпульсів 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 другий лічильник імпульсів виконано як лічильник зі змінним коефіцієнтом ділення, а інформаційні входи цього лічильника підключені до проміжних виходів регістра зсуву у довільному порядку.



Комп'ютерна верстка А. Рябко

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