



УКРАЇНА

(19) UA

(11) 96654

(13) C2

(51) МПК (2011.01)

G06F 7/58 (2006.01)

G07C 15/00

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИОПИС
ДО ПАТЕНТУ НА ВИНАХІД

(54) НЕДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ БІТІВ

1

(21) а201002572

(22) 09.03.2010

(24) 25.11.2011

(46) 25.11.2011, Бюл.№ 22, 2011 р.

(72) ТОРБА АЛЕКСАНДР АЛЕКСЕЄВИЧ, БОБУХ
ВСЕВОЛОД АНАТОЛІЙОВИЧ, ТОРБА ГАННА
ОЛЕКСАНДРІВНА, ГОРБЕНКО ЮРІЙ ІВАНОВИЧ,
ЕЛАКОВ СЕРГІЙ ГЕННАДІЙОВИЧ(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИ-
ТЕТ РАДІОЕЛЕКТРОНІКИ

(56) UA 86979 C2; 10.06.2009

UA 86934 C2; 10.06.2009

JP 64000811 A; 05.01.1989

WO 9748462 A1; 24.12.1997

UA 50386 A; 15.10.2002

UA 68912 A; 16.08.2004

US 2003219119 A1; 27.11.2003

JP 10078864 A; 24.03.1998

JP 2007207054 A; 16.08.2007

GB 2457238 A; 12.08.2009

(57) Недетермінований генератор рівномірно роз-
поділених випадкових бітів, що містить n джерел
ентропії, підключених до перших входів n елемен-
тів «ВИКЛЮЧНЕ АБО», виходи яких з'єднані з вхо-
дами регістра зсуву, поділеного на n частин, а

2

останні виходи кожної частини регістра зсуву під-
ключені до других входів наступних елементів «ВИ-
КЛЮЧНЕ АБО», тактовий генератор, вихід якого
з'єднаний з синхровходами регістра зсуву, який
відрізняється тим, що додатково введені вихід-
ний елемент «ВИКЛЮЧНЕ АБО», перший та дру-
гий лічильники імпульсів, перший та другий парал-
ельні регістри, перший та другий
мультиплексори, інформаційні входи яких підклю-
чені до проміжних виходів регістра зсуву, а виходи
двох мультиплексорів з'єднані з другим та третім
входами першого елемента «ВИКЛЮЧНЕ АБО»,
адресні входи першого та другого мультиплексорів
підключені до виходів відповідно першого та дру-
гого паралельних регістрів, інформаційні входи
яких з'єднані з проміжними виходами регістра зсу-
ву, входи синхронізації першого та другого парал-
ельних регістрів підключені відповідно до виходів
першого та другого лічильників імпульсів, входи
яких з'єднані з виходом тактового генератора, ви-
хід тактового генератора є виходом синхросигналу
пристрою, входи додаткового елемента «ВИКЛЮ-
ЧНЕ АБО» підключені до проміжних виходів регі-
стра зсуву, а вихід цього елемента «ВИКЛЮЧНЕ
АБО» є виходом пристрою.

Винахід належить до області обчислювальної
техніки і може бути використаний в системах захи-
сту інформації обчислювальних систем, напри-
клад, при генерації параметрів алгоритмів крипто-
графічного 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 пос-
ледовательностей на основе физических датчиков
// Радиотехника. Всеукр. між-від. наук.-техн. зб.
2001. Вип. 119, с. 108-113), що містить вузол гене-
рації випадкових логічних рівнів, який складається
з послідовно з'єднаних генератора шуму (фізично-
го датчика шуму), підсилювача-обмежувача та
лічильного триггера, вихід якого з'єднано з входом

дворозрядного регістра зсуву, виходи якого уві-
мкнуті до входів схеми "ВИКЛЮЧНЕ АБО", а вихід
цього елемента з'єднано з входом даних вихідного
регістра зсуву, виходи якого є виходами генерато-
ра 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 швид-
кість 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 вирів-
нюються, а навпаки, ще більше розрізняються за
рахунок статистичного зв'язку між логічними рів-
нями на входах схеми "ВИКЛЮЧНЕ АБО".

(13) C2

(11) 96654

(19) UA

Недоліком цього генератора також є невідповідність спеціальним вимогам стандарту ISO/IEC18031: 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, з метою виводу випадкових послідовностей до ПЕОМ у паралельному форматі 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 виходом запиту переривання ПЕОМ і через буферний елемент "І" з шиною даних ПЕОМ, та дешифратор адреси, включений виходами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного регістра і входу скидання тригера "прапора", і другим виходом до буферного елемента "І".

У послідовному форматі випадкові біти можуть бути зчитані зовнішнім пристроєм з будь-якого виходу регістра зсуву.

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

В основу винаходу поставлена задача створення такого недетермінованого генератора рівномірно розподілених випадкових бітів, в якому додавання нових схемних елементів і зв'язків дозволило б підвищити криптостійкість за рахунок неможливості розрахунку параметрів рекурентного регістра із спостережень та аналізу вихідних випадкових бітів.

Такий технічний результат може бути досягнутий, якщо в недетермінованому генераторі рівномірно розподілених випадкових бітів, 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", тактовий генератор, вихід якого

з'єднаний з синхровходами регістра зсуву, згідно з винаходом додатково введені вихідний елемент "ВИКЛЮЧНЕ АБО", перший та другий лічильники імпульсів, перший та другий паралельні регістри, перший та другий мультиплексори, інформаційні входи яких підключені до проміжних виходів регістра зсуву, а виходи двох мультиплексорів з'єднані з другим та третім входами першого елемента "ВИКЛЮЧНЕ АБО", адресні входи першого та другого мультиплексорів підключені до виходів відповідно першого та другого паралельних регістрів, інформаційні входи яких з'єднані з проміжними виходами регістра зсуву, входи синхронізації першого та другого паралельних регістрів підключені відповідно до виходів першого та другого лічильників імпульсів, входи яких з'єднані з виходом тактового генератора, вихід тактового генератора є виходом синхросигналу пристрою, входи додаткового елемента "ВИКЛЮЧНЕ АБО" підключені до проміжних виходів регістра зсуву, а вихід цього елемента "ВИКЛЮЧНЕ АБО" є виходом пристрою.

Таким чином, введення в недетермінований генератор рівномірно розподілених випадкових бітів додаткового елемента "ВИКЛЮЧНЕ АБО", першого та другого лічильників імпульсів, першого та другого паралельних регістрів, першого та другого мультиплексорів та додавання нових зв'язків дозволяє постійно змінювати параметри рекуренти і за рахунок цього підвищити криптостійкість випадкових бітів, що генеруються, та значно ускладнити процес криптоаналізу цих бітів.

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

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

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 та третій входи першого елемента 2-1 "ВИКЛЮЧНЕ АБО" з'єднані з виходами першого 4 та другого 5 мультиплексорів, інформаційні входи яких підключені до проміжних виходів регістра 3-1...3- n зсуву, адресні входи першого 4 та другого 5 мультиплексорів з'єднані з виходами першого 6 та другого 7 паралельних регістрів, інформаційні входи яких підключені до проміжних виходів регістра 3-1...3- n зсуву, синхровходи першого 6 та другого 7 паралельних регістрів підключені відповідно до виходів першого 8 та другого 9 лічильників імпульсів, тактовий генератор 10, вихід якого є з'єднано з синхровходами регістра 3-1...3- n зсуву, першого 8 та другого 9 лічильника імпульсів та виходом синхросигналу пристрою, додатковий елемент 11 "ВИКЛЮЧНЕ АБО", входи якого підключені до проміжних виходів регістра 3-1...3- n зсуву, а вихід цього елемента 11 "ВИКЛЮЧНЕ АБО" є виходом пристрою.

Недетермінований генератор рівномірно розподілених випадкових бітів працює наступним чином.

На виходах джерел 1-1...1-н 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-н зсуву до входів наступних частин цього регістру, в випадкові моменти часу за допомогою елементів 2-1...2-н "ВИКЛЮЧНЕ АБО". Тактовий генератор 10 формує частоту зсуву випадкових бітів в регістрі 3-1...3-н і таким чином визначає швидкість формування випадкових бітових послідовностей, які за рахунок дії джерел 1-1...1-н ентропії стають непередбачуваними, тобто - недетермінованими, непрогнозованими.

Перший 4 та другий 5 мультиплексори формують сигнали зворотного зв'язку лінійного рекурентного регістра 3-1...3-н зсуву. Логічні рівні з проміжних виходів регістра 3-1...3-н зсуву в випадковому порядку надходять через перший 4 та другий 5 мультиплексори до входів першого елемента 2-1 "ВИКЛЮЧНЕ АБО" та визначають параметри рекуренти. Випадковий характер комутації сигналів мультиплексорами 4, 5 визначається логічними рівнями на їх адресних входах, які підключені до виходів першого 6 та другого 7 паралельних регістрів. Ці регістри запам'ятовують випадкові сигнали з проміжних виходів регістра 3-1...3-н зсуву. Часові

інтервали зміни сигналів в першому паралельному регістрі 6 визначаються першим лічильником 8 імпульсів, а в другому паралельному регістрі 7 - другим лічильником 9 імпульсів. Входи лічильників 8, 9 імпульсів підключені до виходу тактового генератора 10. Коефіцієнти ділення лічильників імпульсів 8, 9 повинні бути взаємно простими.

Логічні сигнали з проміжних виходів регістра 3-1...3-н зсуву об'єднуються елементом 11 "ВИКЛЮЧНЕ АБО", вихід якого є виходом пристрою. Недетерміновані випадкові біти зчитуються зовнішнім пристроєм з виходу елемента 11 "ВИКЛЮЧНЕ АБО" по фронтам синхросигнала з виходу тактового генератора 10.

На відміну від пристрою-прототипу (див. патент України №50386 А, МПК6 G06F7/58, G07C15/00, опублікований 15.10.2002, Бюл. №10), у якому параметри рекуренти, а саме: довжина регістра зсуву і номер проміжного виходу регістра зсуву для зворотного зв'язку є незмінними впродовж усього часу роботи пристрою, у заявленому недетермінованому генераторі рівномірно розподілених випадкових бітів обидва параметри рекуренти постійно змінюються у випадковому порядку. Навіть при повному збої джерел 1-1...1-н ентропії криптостійкість пристрою задовольняє вимоги стандарту ISO/IEC18031:2005, тому що математичний розрахунок параметрів рекуренти регістра 3-1...3-н зсуву при спостереженні вихідних бітів є неможливим.

