



УКРАЇНА

(19) **UA** (11) **99018** (13) **C2**
(51) МПК (2012.01)
G06F 7/00
G07C 15/00

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

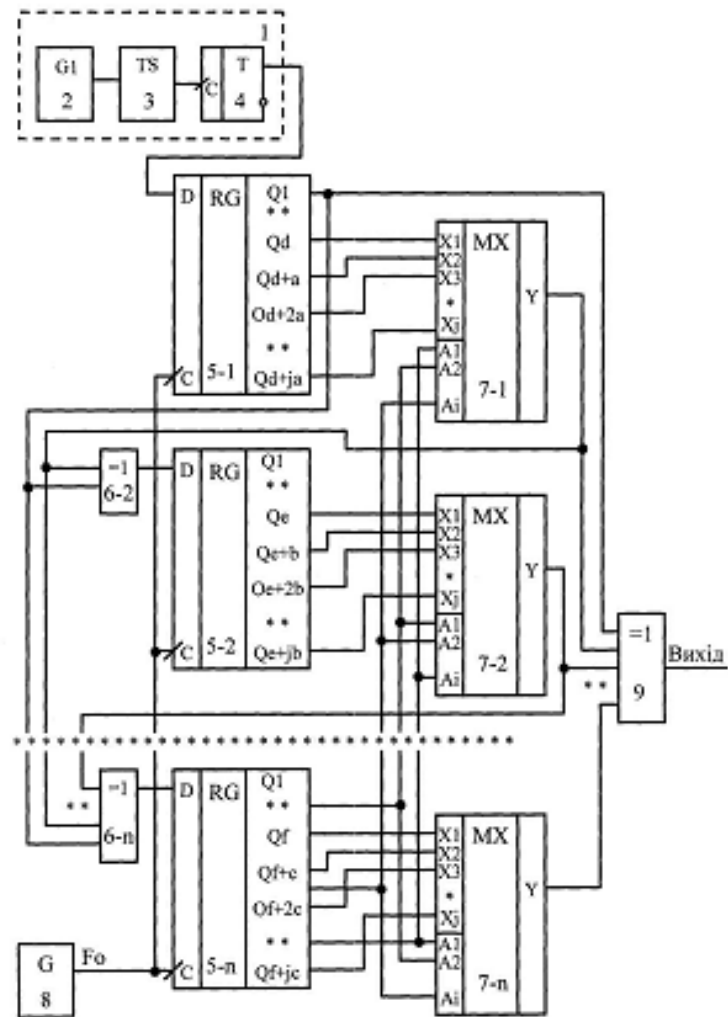
(21) Номер заявки: а 2010 13769	(72) Винахідник(и): Торба Александр Алексеевич (UA), Бобух Всеволод Анатолійович (UA), Бобкова Анна Александровна (UA), Єлаков Сергій Геннадійович (UA)
(22) Дата подання заявки: 19.11.2010	(73) Власник(и): ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ, пр. Леніна, 14, м. Харків, 61166, Україна (UA)
(24) Дата, з якої є чинними права на винахід: 10.07.2012	(56) Перелік документів, взятих до уваги експертизою: UA 61439 A; 17.11.2003 UA 82252 C2; 25.03.2008 UA 86979 C2; 10.06.2009 SU 1599856 A1; 15.10.1990 JP 2007179524 A; 12.07.2007 JP 57045645 A; 15.03.1982 WO 2009063948 A1; 22.05.2009 GB 2457238 A; 12.08.2009
(41) Публікація відомостей про заявку: 25.05.2012, Бюл.№ 10	
(46) Публікація відомостей про видачу патенту: 10.07.2012, Бюл.№ 13	

(54) ГЕНЕРАТОР РІВНОМІРНО РОЗПОДІЛЕНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

(57) Реферат:

Генератор рівномірно розподілених випадкових послідовностей належить до обчислювальної техніки, а саме до систем захисту інформації. Генератор містить вузол генерації випадкових логічних рівнів, який складається з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, регістри зсуву, елементи "ВИКЛЮЧНЕ АБО", тактовий генератор. Додатково введені n-1 регістрів зсуву, n мультиплексорів та n-1 елементів "ВИКЛЮЧНЕ АБО". Технічним результатом є підвищення швидкості формування випадкових послідовностей і покращення їх статистичних характеристик.

UA 99018 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. 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".

Найбільш близьким по сукупності ознак є генератор рівномірно розподілених випадкових послідовностей (Патент України № 6143 9А, МПК7 G06F7/58, G07C15/00, опублік. 17.11.2003, Бюл. №11), що містить вузол генерації випадкових логічних рівнів, який складається з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, вихід якого з'єднаний з входом багаторозрядного регістра зсуву, а його виходи підключені до входів елемента "ВИКЛЮЧНЕ АБО", на виході цього елемента формуються послідовності випадкових бітів, які за допомогою вихідного регістра зсуву перетворюються в паралельний формат.

Недоліком цього генератора є невелика швидкість формування випадкових послідовностей, тому що до входів елемента "ВИКЛЮЧНЕ АБО" надходять з декількох виходів регістра зсуву послідовності випадкових сусідніх бітів, які мають значні кореляційні зв'язки між собою.

В основу винаходу поставлена задача створення такого генератора рівномірно розподілених випадкових послідовностей, в якому додавання нових схемних елементів і зв'язків дозволило б підвищити швидкість формування випадкових бітових послідовностей за рахунок зменшення кореляційних зв'язків між сусідніми бітами.

Такий технічний результат може бути досягнутий, якщо в генераторі рівномірно розподілених випадкових послідовностей, що містить вузол генерації випадкових логічних рівнів, який складається з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, а його вихід підключено до входу регістра зсуву, перший вихід якого з'єднаний з першим входом елемента "ВИКЛЮЧНЕ АБО", вихід якого є виходом пристрою, тактовий генератор з'єднаний виходом з синхровходом регістра зсуву, згідно з винаходом, додатково введені $n-1$ регістрів зсуву, n мультиплексорів та $n-1$ елементів "ВИКЛЮЧНЕ АБО", виходи регістрів зсуву підключені до інформаційних входів мультиплексорів, виходи яких з'єднані з входами вихідного елемента "ВИКЛЮЧНЕ АБО", адресні входи мультиплексорів підключені до виходів останнього регістра зсуву у довільному порядку, а входи додаткових регістрів зсуву з'єднані з виходами додаткових елементів "ВИКЛЮЧНЕ АБО", входи яких підключені до першого виходу першого регістра зсуву а також до виходів усіх попередніх мультиплексорів, синхровходи додаткових регістрів зсуву підключені до виходу тактового генератора.

Таким чином, введення в генератор рівномірно розподілених випадкових послідовностей додаткових регістрів зсуву, мультиплексорів та елементів "ВИКЛЮЧНЕ АБО" дозволяє усунути статистичну залежність між сусідніми бітами на виходах мультиплексорів за рахунок випадкової комутації сигналів з різних виходів регістра зсуву і таким чином підвищити швидкодію генератора випадкових бітів і покращити статистичні характеристики бітових послідовностей, що генеруються.

На кресленні зображена структурна схема генератора рівномірно розподілених випадкових послідовностей.

На кресленні використані наступні міжнародні позначення: G - генератор, TS - тригер Шмітта, T - тригер, RG - регістр, MX - мультиплексор.

Генератор містить вузол 1 генерації випадкових логічних рівнів, який складається з послідовно з'єднаних генератора 2 шуму, підсилювача-обмежувача 3 і лічильного тригера 4, вихід якого з'єднаний з інформаційним входом першого регістра 5-1 зсуву. Інформаційні входи

наступних регістрів 5-2...5-n зсуву з'єднані з виходами елементів 6-2...6-n "ВИКЛЮЧНЕ АБО", входи яких підключені до першого виходу першого регістра 5-1 зсуву та до виходів усіх попередніх мультиплексорів 7-1...7-n. Синхровходи регістрів 5-1...5-n зсуву з'єднані з виходом тактового генератора 8, а входи цих регістрів 5-1...5-n зсуву підключені до інформаційних входів мультиплексорів 7-1...7-n. Адресні входи мультиплексорів 7-1...7-n з'єднані з виходами останнього регістра 5-n зсуву у довільному порядку. Перший вихід першого регістра 5-1 зсуву а також входи мультиплексорів 7-1...7-n підключені до виходів вихідного елемента 9 "ВИКЛЮЧНЕ АБО", вихід якого є виходом пристрою.

Генератор рівномірно розподілених випадкових послідовностей працює наступним чином. На виході генератора 2 шуму формуються імпульси випадкової амплітуди, наступні через випадкові часові інтервали. Ці випадкові імпульси підсилювачем-обмежувачем 3 перетворюються в логічні рівні цифрових мікросхем. Імпульси з виходу підсилювача-обмежувача 3 подаються на вхід лічильного тригера 4, на виході якого формуються логічні рівні, з рівною імовірністю приймаючи значення нуля або одиниці в випадкові моменти часу.

Випадкові логічні рівні з виходу лічильного тригера 4 записуються в регістр 5-1 зсуву з частотою F_0 , що визначається тактовим генератором 8. Випадкові логічні рівні на виходах регістра 5-1 зсунуті у часі на відстань, кратну періоду тактового генератора 8. Через декілька розрядів регістра 5-1 зсуву, тобто через декілька часових інтервалів тактової частоти F_0 кореляційні зв'язки між випадковими логічними рівнями зменшуються. Мультиплексор 7-1 вибирає у випадковому порядку логічні рівні, з меншою статистичною залежністю, ніж на вході регістра 5-1 зсуву, та комутує (тобто передає) до входу елемента 9 "ВИКЛЮЧНЕ АБО", вихід якого є виходом пристрою.

На входи наступних регістрів 5-2...5-n зсуву випадкові логічні рівні подаються через елементи 6-2...6-n "ВИКЛЮЧНЕ АБО", входи яких підключені до першого виходу першого регістра 5-1 зсуву та до виходів усіх попередніх мультиплексорів 7-1...7-n. Тому на входах кожного регістра 5-2...5-n зсуву статистична залежність між сусідніми випадковими рівнями значно зменшується. Логічні рівні на виходах усіх наступних регістрів 5-2...5-n зсуву аналогічно комутуються мультиплексорами 7-2...7-n до входів елемента 9 "ВИКЛЮЧНЕ АБО".

Логічні рівні на виходах останнього регістра 5-n зсуву мають найменші статистичні зв'язки, і тому їх можливо подавати як випадкові коди на адресні входи мультиплексорів 7-2...7-n у довільному порядку.

Кількість розрядів між виходами регістрів 5-1...5-n поступово зменшується таким чином, щоб зменшити статистичну залежність між логічними рівнями на сусідніх входах мультиплексорів 7-1...7-n. Це сприяє покращенню статистичних характеристик випадкових послідовностей, які генеруються.

ФОРМУЛА ВИНАХОДУ

Генератор рівномірно розподілених випадкових послідовностей, що містить вузол генерації випадкових логічних рівнів, який складається з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, а вихід вузла підключено до входу регістра зсуву, перший вихід якого з'єднаний з першим входом елемента "ВИКЛЮЧНЕ АБО", вихід якого є виходом пристрою, тактовий генератор з'єднаний виходом з синхровходом регістра зсуву, який **відрізняється** тим, що додатково введені n-1 регістрів зсуву, n мультиплексорів та n-1 елементів "ВИКЛЮЧНЕ АБО", входи регістрів зсуву підключені до інформаційних входів мультиплексорів, входи яких з'єднані з входами вихідного елемента "ВИКЛЮЧНЕ АБО", адресні входи мультиплексорів підключені до виходів останнього регістра зсуву у довільному порядку, а входи додаткових регістрів зсуву з'єднані з виходами додаткових елементів "ВИКЛЮЧНЕ АБО", входи яких підключені до першого виходу першого регістра зсуву, а також до виходів усіх попередніх мультиплексорів, синхровходи додаткових регістрів зсуву підключені до виходу тактового генератора.

