УКРАЇНА

(19) UA (11) 47876 (13) U

(51) МПК (2009)
G06F 7/58

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

(21) u200909574
(22) 18.09.2009
(24) 25.02.2010
(46) 25.02.2010, Бюл.№ 4, 2010 р.
(72) РИСОВАНИЙ ОЛЕКСАНДР МИКОЛАЙОВИЧ, КОЛОМІЙЦЕВ ОЛЕКСІЙ ВОЛОДИМИРОВИЧ, ГОГОТОВ ВАЛЕРІЙ ВАСИЛЬОВИЧ
(73) НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
(57) Генератор псевдовипадкової послідовності, що містить комутатор для вибору зворотних зв'язків, який **відрізняється** тим, що в нього введені дворозрядні регістри, схеми множення на два за модулем три та суматор за модулем три, при цьому виходи суматора за модулем три підключаються до молодшого дворозрядного регістра, виходи якого підключаються до однойменних входів схем множення на два за модулем три, виходи яких підключаються як до однойменних входів наступного дворозрядного регістра, так й до входів комутатора, виходи яких підключаються до входів суматора за модулем три.

1

Корисна модель належить до обчислювальної техніки та може використовуватися у системах діагностування цифрових об'єктів.

Відомий пристрій [Авт. св. СССР №1465885. 1989. Бюл. №10. Генератор псевдослучайной последовательности. Іванов М.А.], який містить на кожен розряд послідовності два блоки перемноження, один суматор в полі GF(L), двохрозрядний регістр та дешифратор, який є загальним для всіх розрядів послідовності. Недоліком такого пристрою є складність за рахунок використання дешифратора та великої кількості зв'язків з виходів кожного регістра до входів цього дешифратора для аналізу визначених комбінацій ПОСЛІДОВНОСТІ, яка формується.

Найбільш близьким до того, що пропонується технічним рішенням, вибраним як прототип, є пристрій [Авт. св. СССР №1539774. 1990. Бюл. №4. Генератор псевдослучайной последовательности. Батраченко В.С., Сошников Э.Н.], який містить генератор тактових імпульсів, реверсивний регістр зсуву, перший та другий суматори за модулем два, перший та другий елементи І, комутатор, дільник частоти та Т-тригер. Недоліком такого пристрою є невелика довжина псевдовипадкової послідовності за рахунок використання суматорів за модулем два.

В основу корисної моделі поставлено задачу розширення функціональних можливостей генератора за рахунок збільшення довжини псевдовипадкової послідовності, яка. Досягається при використанні суматора за модулем три.

2

Задача вирішується тим, що у генератор псевдовипадкової послідовності який містить комутатор для вибору зворотних зв'язків додатково введені дворозрядні регістри, схеми множення на два за модулем три та суматор за модулем три, при ньому виходи суматора за модулем три підключаються до молодшого дворозрядного регістра, гаї ходи якого підключаються до однойменних входів схем множення на два за модулем три, виходи яких підключаються як до однойменних входів наступного дворозрядного регістра так й до входів комутатора, виходи яких підключаються до входів суматора за модулем три.

Позитивним технічним результатом є те, що отримано пристрій, який дозволяє збільшити довжину псевдовипадкової послідовності, яку він формує.

При пошуку в патентній та науково-технічній літературі не виявлено об'єктів з ознаками, подібними до відмінних ознак технічного рішення, що заявляється, на підставі чого можна зробити висновок про відповідність його критерію "суттєві відмінності".

Генератор псевдовипадкової послідовності реалізує метод формування псевдовипадкової послідовності з використанням регістрів зсуву з суматором за модулем три в ланцюгу зворотного зв'язку.

На Фіг.1 наведена структурна схема пристрою в загальному вигляді. Пристрій включає: групу блоків $1_1 - 1_n$ дворозрядних регістрів, кількість яких дорівнює максимальній ступені утворюючого полі-

(19) UA (11) 47876 (13) U

нома; групу блоків 2_1-2_n множення на два за модулем три; комутатор 3 та схему суматора 4 на два за модулем три, де n - максимальна ступень утворюючого полінома $p(x)=\alpha_n X^n \oplus_3 \ldots \oplus_3 \alpha_i X^i \alpha_1 \oplus_3 \alpha_1 X \oplus_3 \alpha_0$ - примітивного над полем GF(3). Величина α_i, на яку виконується множення в блоці множення відповідного дворозрядного регістра відзначається відповідним елементом квадратної матриці зв'язків *S,* яка Tl кінцевому полі GF(3*)* має вигляд:

$$S=\begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_i & \ldots & \alpha_n \\ 1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 \\ \ldots & & & \ldots & & \ldots \\ 0 & 0 & \ldots & 0 & \ldots & 1 \end{vmatrix}$$

та описує з'єднання виходів та входів блоків 1_1-1_n дворозрядних регістрів пристрою, де - α_i {0, 1,2}.

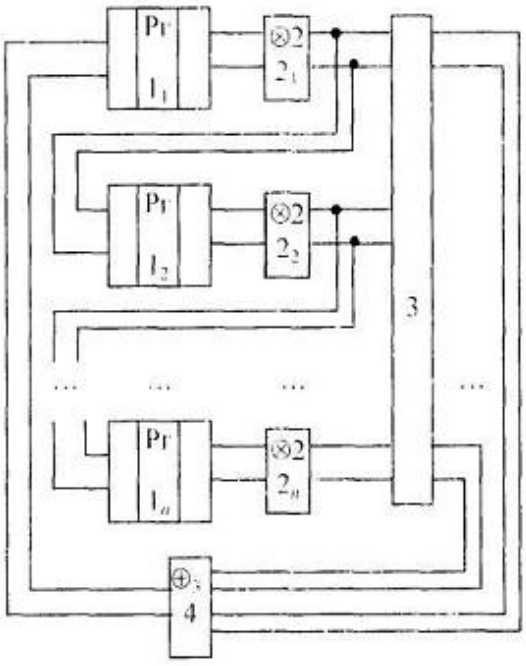
Якщо елемент α_i матриці зв'язків S відсутній, то зв'язок між відповідним дворозрядним регістром l_i, та схемою суматора 4 на два за модулем три відсутній.

Множення на коефіцієнт 2 в блоці множення відбувається, якщо $\alpha_i = 2$.

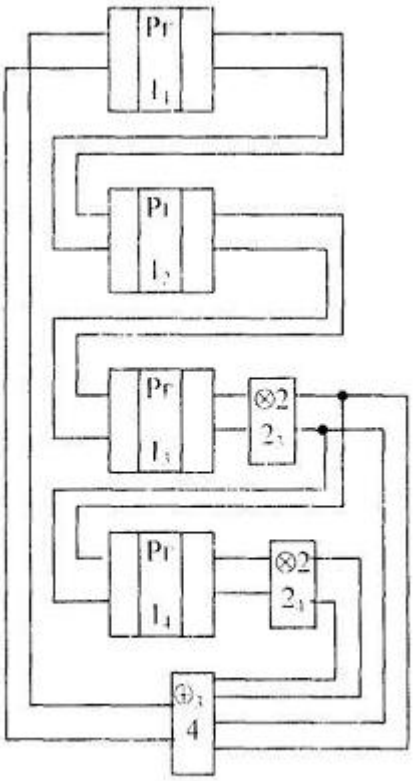
На схемі не показані входи встановлення пристрою в початковий стан, ланцюги синхронізації та виходи псевдовипадкової послідовності. Перед початком роботи всі регістри пристрою встановлюються в початковий стан, який може бути довільним. Прихід кожного тактового імпульсу викликає зсув вмісту дворозрядних регістрів 2_1-2_n пристрою праворуч з одночасним записуванням нового значення в молодший розряд дворозрядного регістра. Вкачане нове значення, поступає з виходів суматора 4 за модулем три, входи якого з'єднуються з виходами комутатора 3. Наявність або відсутність виходів з комутатора 3 визначаються виглядом утворюючого полінома P(x).

На Фіг.2 наведена схема генератора псевдовипадкової послідовності, вигляд зворотних зв'язків якого відповідає утворюючому поліному $P(x)=2X^4 \oplus_3 2X^3 \oplus_3 1$.В даному випадку схема комутатора 3 перетворюється в ланцюги з'єднання виходів дворозрядного регістра або схем множення з входами суматора за модулем три.

Якщо використати поліном четвертого ступеня, то довжина одного циклу генерації пристрою, який вибрано в якості прототипу, буде дорівнювати 2^4-1, а один цикл генерації пропонованого пристрою буде дорівнювати 3^4-1, чим й досягається мета корисної моделі.



Фіг. 1



Фіг. 2

Комп'ютерна верстка А. Крижанівський Підписне Тираж 26 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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