



УКРАЇНА

(19) UA (11) 66502 (13) U
(51) МПК
G06F 7/58 (2006.01)ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬвидається під
відповідальність
власника
патенту

(54) ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ В КІНЦЕВОМУ ПОЛІ GF(3)

1

2

(21) u201106772

(22) 30.05.2011

(24) 10.01.2012

(46) 10.01.2012, Бюл.№ 1, 2012 р.

(72) РИСОВАНІЙ ОЛЕКСАНДР МИКОЛАЙОВИЧ,
ЛИТОВСЬКИЙ ВІТАЛІЙ ДМИТРОВИЧ, КОЗІНА
ОЛЬГА АНДРІЙВНА, ШОСТАК АНАТОЛІЙ ВАСИ-
ЛЬОВИЧ(73) НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"(57) Генератор псевдовипадкових послідовностей
в кінцевому полі GF(3), що містить групу блоків
дворозрядних регістрів, кількість яких дорівнює
максимальному ступеню утворюючого полінома,

комутатор та схему суматора за модулем три, який **відрізняється** тим, що в нього введені блоки множення на два у вигляді перехресних ліній передачі даних, 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, які виконані у вигляді перехресних ліній передачі даних, виходи яких підключаються як до однойменних входів наступного дворозрядного регістра, так й до входів комутатора, виходи яких підключаються до входів суматора за модулем три.

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

Відомий генератор псевдовипадкових послідовностей [1], який містить на кожен розряд послідовності два блоки перемноження, один суматор в полі GF(L), дворозрядний 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 генератор [2].

Недоліком відомого генератора є надмірна кількість логічних елементів.

В основу корисної моделі поставлена задача спрощення пристрою за рахунок спрощення блоків множення на два за модулем три.

Задача вирішується тим, що у відомий генератор псевдовипадкових послідовностей, який містить групу блоків дворозрядних регістрів, кількість яких дорівнює максимальному ступеню утворюючого полінома; комутатор та схему суматора за модулем три додатково введені блоки множення на два, які виконані у вигляді перехресних ліній передачі даних. Фізично цих блоків не існує, а є тільки перехресні лінії. Цей результат досягається

при використанні наступної логіки дешифрування трійкового сигналу:

Входи	Виходи
0	00
1	01
X	10

Знаком x позначено третій (високий) стан.

Позитивним технічним результатом є те, що отримано пристрій з меншою кількістю логічних елементів. Якщо при побудові генератора використано поліном

$$P(x) = a_r x^r \oplus_3 a_{r-1} x^{r-1} \oplus_3 \dots \oplus_3 a_1 x^1 \oplus_3 a_0$$

примітивного над кінцевим полем GF(3) з всіма $a_i = 2$, то число таких блоків зменшується в 2 рази.

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 висновки про відповідність його критерію "суттєві відмінності".

На Фіг. 1 наведена схема генератора псевдовипадкових послідовностей по модулю три. Пристрій включає: групу блоків $1_1 - 1_n$ дворозрядних регістрів; групу блоків $2_1 - 2_n$ множення на два за модулем три, які виконані у вигляді перехресних

(13) U

(11) 66502

(19) UA

ліній передачі даних; комутатор 3, схему суматора 4 за модулем три та пари вихідних сигналів $S_1 - S_n$ псевдовипадкової послідовності.

Генератор є схемою, що здійснює зсув вмісту регістру з урахуванням зворотних зв'язків, які вибираються у відповідності до утворюючого характеристичного полінома

$P(x) = a_r x^r \oplus a_{r-1} x^{r-1} \oplus \dots \oplus a_1 x \oplus a_0$, примітивного над кінцевим полем $GF(3)$. Вільний член характеристичного утворюючого полінома a_0 впливає на вигляд матриці станів та не залежить від зв'язків регістра зсуву, які задаються матрицею зв'язків:

$$S = \begin{pmatrix} a_1 & a_2 & \dots & a_{r-1} & a_r \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix},$$

де $r = \deg P(x)$.

Вектор наступного стану регістра можна визначити з виразу:

$$h_k^T = S \times h_{k-1}^T,$$

де k - поточний номер такту;

T - символ транспонування.

Наприклад,

$$h_2^T = S \times h_1^T, h_3^T = S^2 \times h_1^T.$$

Тоді, через k тактів

$$h_k^T = S^{k-1} \times h_1^T.$$

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

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

На схемі не показані входи встановлення пристрою в початковий стан та ланцюги синхронізації.

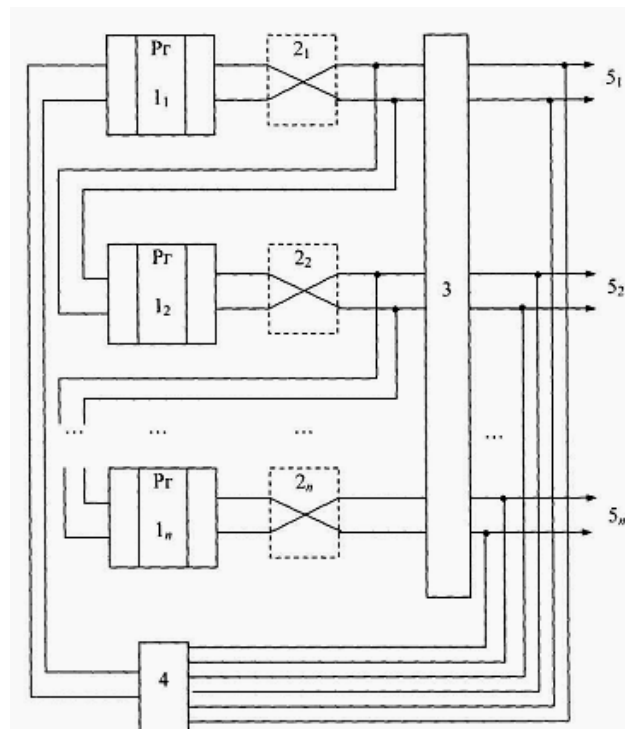
На Фіг.2 наведена схема генератора псевдовипадкової послідовності, вигляд зворотних зв'язків якого відповідає утворюючому поліному

$P(x) = 2x^4 \oplus 2x^3 \oplus 1$. В даному випадку схема комутатора 3 перетворюється в ланцюги з'єднання виходів дворозрядного регістра або схем множення на два за модулем три, які виконані у вигляді перехресних ліній передачі даних зі входами суматора за модулем три. Якщо біля показника ступеня у вигляді полінома знаходиться двійка, то це позначає, що замість блока множення на два за модулем три використовується перехресна передача сигналів, яка й виконує множення на два за модулем три, чим й вирішується задача корисної моделі.

Джерела інформації:

1. Авторское свидетельство СССР № 1465885, кл. G06F7/58, 1989.

2. Патент України на корисну модель № 47876, Україна, МПК G06F7/58. Генератор псевдовипадкових послідовностей / О.М. Рисований, О.В. Коломійцев, В.В. Гоготов. - № U2009 09574; Заяв. 18.09.2009; Опубл. 25.02.2010; Бюл. №4.-6 с. (прототип).



Фіг. 1

