



УКРАЇНА

(19) UA (11) 25491 (13) U
(51) МПК
G06F 7/49 (2007.01)МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬвидається під
відповідальність
власника
патенту(54) ПРИСТРІЙ ДЛЯ МНОЖЕННЯ ЕЛЕМЕНТІВ СКІНЧЕНИХ ПОЛІВ $GF(2^n)$

1

2

(21) u200703644

(22) 02.04.2007

(24) 10.08.2007

(46) 10.08.2007, Бюл. № 12, 2007 р.

(72) Жуков Ігор Анатолійович, Кубицкий Володи-
мир Іванович, Синельников Олексій Олексійович

(73) НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

(57) Пристрій для множення елементів скінчених полів $GF(2^n)$, який містить блок формування часткових добутоків, що складається з n груп по n елементів l у кожній, $(n-1)$ блоків матричного перетворення та блок додавання, виходи якого з'єднані з виходом результату пристрою, вхід 1-го розряду першого $(l=1, \dots, n)$ співмножника якого з'єднаний з згрупованими першими входами елементів l i -ої групи блока формування часткових добутоків, входи поточної суми j -го блока матричного перетворення $(j=2, \dots, n-1)$ з'єднані з виходами поточної суми $(j-1)$ -го блока матричного перетворення, який відрізняється тим, що в нього введений дешифратор, а кожний блок матричного перетворення містить першу і другу групи із n та $(n-1)$ суматорів по модулю два, першу і другу групи з $(n-2)$ та n елементів l та елемент АБО, причому входи дешифратора з'єднані з відповідними входами коефіцієнтів утворюючого полінома пристрою і входами коефіцієнтів утворюючого полінома кожного з $(n-1)$ блоків матричного перетворення, а виходи - зі входами коефіцієнтів розширення k -го блока матричного перетворення $(k=1, \dots, n-2)$, виходи поточної суми $(n-1)$ -го блока матричного перетво-

рення з'єднані з першими входами блока додавання, другі входи якого з'єднані з виходами відповідних елементів l з першої по $(n-1)$ групи блока формування часткових добутоків якого з'єднані відповідно з входами часткових добутоків з першого по $(n-1)$ блок матричного перетворення, вхід i -го розряду другого співмножника пристрою з'єднаний з групованими другими входами i -их елементів l в кожній групі блока формування часткових добутоків, при цьому в кожному блоці матричного перетворення перші входи суматорів по модулю два першої групи з'єднані з входами поточної суми блока, входи часткових добутоків якого з'єднані з другими входами суматорів по модулю два першої групи, виходи яких, починаючи з другого, з'єднані відповідно з першими входами суматорів по модулю два другої групи, другі входи яких з'єднані з виходами з першого по $(n-1)$ -ий елемент l другої групи, виходи суматорів по модулю два та вихід $(n-2)$ -го елемента l другої групи з'єднані з відповідними виходами поточної суми блока, виходи суматорів по модулю два з першого по $(n-2)$ -ий першої групи з'єднані відповідно з першими входами елементів l першої групи, другі входи яких з'єднані з відповідними входами коефіцієнтів розширення блока, а виходи - з входами елемента АБО, вихід якого з'єднаний з групованими першими входами елемента l другої групи, другі входи яких з'єднані з відповідними входами коефіцієнтів утворюючого полінома блока.

Корисна модель належить до галузі обчислювальної техніки і може бути використана в пристроях для кодування та декодування циклічних кодів, призначених для передачі повідомлень з високою достовірністю в системах доставки і обробки дискретної інформації.

Відомий пристрій для множення елементів скінчених полів, що містить блок множення на старший розряд та a_{i-1} блоків обчислення поліномів, блок зсуву співмножника, блок завдання зворотних

зв'язків, блок формування величини зсуву та блок зсуву добутку [1].

Такі пристрої мають великі апаратні витрати в цілому та на реалізацію схем контролю і схем видачі результату.

Найбільш близьким до пропонованого по технічній суті є [2] пристрій для множення елементів скінчених полів $GF(2^n)$, що містить перший та другий регістри, n груп по n елементів l в кожній, n багатовходових суматорів по модулю два і $(n-1)$ блоків матричного перетворення, входи першого і

(13) U

(11) 25491

(19) UA

другого регістрів є входами коефіцієнтів першого і другого співмножників, виходи першого регістру з'єднані з об'єднаними першими входами n елементів I в одноіменних з номерами виходів першого регістру групах елементів I відповідно, а виходи другого регістру під'єднані до одноіменних входів першого блоку матричного перетворення та до других входів одноіменних елементів I першої групи елементів I , при цьому, виходи попередніх блоків матричного перетворення під'єднані до одноіменних входів слідуєчих блоків матричного перетворення та до других входів одноіменних елементів I слідуєчих груп, виходи одноіменних елементів I кожної групи з'єднані з входами, одноіменними з елементами I багатовходових суматорів по модулю два, виходи яких є виходами пристрою.

Недоліком даного пристрою є обмеженість функціональних можливостей.

Задачею корисної моделі є удосконалення пристрою для множення елементів скінченних полів шляхом введення дешифратора.

Це дозволяє забезпечити безпосередньо виконувати множення елементів різноманітних скінчених полів $GF(2^n)$, тобто має широкі функціональні можливості.

Поставлена задача вирішується тим, що в пристрої для множення елементів скінченних полів $GF(2^n)$, який містить блок формування часткових добутків, який складається з n груп по n елементів I кожній, $(n-1)$ блоків матричного перетворення та блок додавання, виходи якого з'єднані з виходом результату пристрою, вхід 1-го розряду першого $(I=1, \dots, n)$ співмножника якого з'єднаний з згрупованими першими входами елементів I i -ої групи блоку формування часткових добутків, входи поточної суми j -го блоку матричного перетворення $(j=2, \dots, n-1)$ з'єднані з виходами поточної суми $(j-1)$ -го блоку матричного перетворення, а також, згідно з корисною моделлю, введено дешифратор, а кожний блок матричного перетворення містить першу і другу групи із n та $(n-1)$ суматорів по модулю два, першу і другу групи з $(n-2)$ та n елементів I та елемент АБО, причому входи дешифратора з'єднані з відповідними входами коефіцієнтів утворюючого поліному пристрою і входами коефіцієнтів утворюючого поліному кожного з $(n-1)$ блоків матричного перетворення, а виходи зі входами коефіцієнтів розширення k -го блоку матричного перетворення $(k=1, \dots, n-2)$, виходи поточної суми $(n-1)$ -го блоку матричного перетворення з'єднані з першими входами блоку додавання, другі входи якого з'єднані з виходами відповідних елементів I з першої по $(n-1)$ блока формування часткових добутків групу якого з'єднані відповідно з входами часткових добутків з першого по $(n-1)$ блок матричного перетворення, вхід i -го розряду другого співмножника пристрою з'єднаний з групованими другими входами i -их елементів I в кожній групі блоку формування часткових добутків, при цьому в кожному блоці матричного перетворення перші входи суматорів по модулю два першої групи з'єднані з входами поточної суми блоку, входи часткових добутків якого з'єднані з другими входами суматорів по модулю два першої групи, виходи яких,

починаючи з другого, з'єднані відповідно з першими входами суматорів по модулю два другої групи, другі входи яких з'єднані з входами з першого по $(n-1)$ -ий елемент I другої групи, виходи суматорів по модулю два та вихід $(n-2)$ -го елементу I другої групи з'єднані з відповідними входами поточної суми блоку, виходи суматорів по модулю два з першого по $(n-2)$ -ий першої групи з'єднані відповідно з першими входами елементів I першої групи, другі входи яких з'єднані з відповідними входами коефіцієнтів розширення блоку, а виходи з входами елемента АБО, вихід якого з'єднаний з групованими першими входами елемента I другої групи, другі входи яких з'єднані з відповідними входами коефіцієнтів утворюючого поліному блоку.

Множення елементів скінчених полів $GF(2^n)$ виконується як множення многочленів та зводиться до обчислення суми часткових добутків з приведенням її по модулю утворюючого поліному, що забезпечує множення елементів скінчених полів $GF(2^n)$ $(2 \leq m \leq n)$, створених різними утворюючими поліномами. В результаті це дозволяє забезпечити безпосередньо виконувати множення елементів різноманітних скінчених полів $GF(2^n)$, і як наслідок, розширюються функціональні можливості.

На Фіг.1 зображена структурна схема пристрою для множення елементів скінчених полів $GF(2^n)$. На Фіг.2 - структурна схема блоку матричного перетворення. На Фіг.3 - структурна схема дешифратора. На Фіг.4 - комбінаційна схема множення скінченого поля $GF(2^n)$. На Фіг.5 - Схема одного $(n-1)$ -го розряду пристрою обчислення операційних коефіцієнтів $p_i^{(j)}$. На Фіг.6 - 1-й рівень комбінаційної схеми множення елементів скінчених полів. На Фіг.7 - універсальна комбінаційна схема множення елементів скінчених полів $GF(2^n)$.

Пристрій для множення елементів скінчених полів містить входи 1 коефіцієнтів утворюючого поліному, входи 2 першого співмножника, входи 3 другого співмножника, блок 4 формування часткових добутків, $(n-1)$ блоків 5 матричного перетворення, блок 6 додавання, дешифратор 7 та виходи 8 результату.

Блок 5 матричного перетворення містить входи 9 поточної суми, входи 10 часткових добутків, входи 11 поточного коефіцієнту розширення, входи 12 коефіцієнтів утворюючого поліному, першу групу з n суматорів 13 по модулю два, першу групу з $(n-2)$ елементів I 14, $(n-2)$ - вхідних елементів АБО 15, другу групу з n елементів I 16, другу групу з $(n-1)$ суматорів 17 по модулю два та виходи поточної суми.

Дешифратор 7 містить входи 19 коефіцієнтів утворюючого поліному, групу з $(n-3)$ інверторів 20, групу з $(n-3)$ елементів I 21 та виходи 22 поточного коефіцієнту розширення.

Пристрій для множення елементів скінчених полів $GF(2^n)$ працює в такий спосіб.

Перед початком множення на входи 1 утворюючого поліному пристрою поступають значення коефіцієнтів утворюючого поліному $g^m(x)$, що призводить до формування на відповідному виході дешифратора 7 коефіцієнта розширення m . При

поданні на входи 2 та 3 пристрою відповідно першого $\overline{a(x)}$ та другого $\overline{b(x)}$ співмножників на виходах блоку 4 формування часткових добутоків утворюються часткові добутки $\overline{a(x)} * b_i$, які подаються на входи 10 часткових добутоків відповідних i -тих блоків 5 матричного перетворення, входи 9 поточної суми кожного з яких з'єднані з одноіменними входами 18 попереднього $(i-1)$ -го блоку 5 матричного перетворення. На виходах 18 кожного i -го блоку 5 матричного перетворення формується i -а поточна сума як приведена по модулю утворюючого поліному сума i -го часткового добутку та $(i-1)$ -ї поточної суми, $\overline{a(x)} * b_i \oplus \overline{P_{n-1}(x)} \bmod g^m(x)$. Таким чином, на виходах 19 $(n-1)$ -го блоку 5 матричного перетворення формується поточна сума $\overline{P_{n-1}(x)}$, як сума $\overline{a(x)} * b_1 \oplus \overline{P_{n-2}(x)} \bmod g^m(x)$. Остаточний результат множення елементів скінчених полів формується на виходах 8 блоку 6 підсумовування.

Блок 4 формування часткових добутоків, який вміщує в себе n груп по n елементів I в кожній, слугує для отримання послідовності часткових добутоків виду $\overline{a(x)} * b_k$, a_i - множина коефіцієнтів першого співмножника, b_k - коефіцієнт другого співмножника. На виходах елементів I перші групи формують часткові добутки $a_{(n-1)} * b_{(n-1)}$, $a_{(n-2)} * b_{(n-1)}$, $a_{(n-3)} * b_{(n-1)}$, ..., $a_1 * b_{(n-1)}$, $a_0 * b_{(n-1)}$, на виходах другої групи елементів I - $a_{(n-1)} * b_{(n-2)}$, $a_{(n-2)} * b_{(n-2)}$, $a_{(n-3)} * b_{(n-2)}$, ..., $a_1 * b_{(n-2)}$, $a_0 * b_{(n-2)}$, на виходах n -ої групи елементів I - $a_{(n-1)} * b_0$, $a_{(n-2)} * b_0$, $a_{(n-3)} * b_0$, ..., $a_1 * b_0$, $a_0 * b_0$.

Дешифратор 7 призначений для визначення коефіцієнта розширення поля. Так, як ступінь розширення поля визначається старшим коефіцієнтом перетворюючого поліному $g^m(x)$, то поява сигналу "1" в старшому коефіцієнті утворюючого поліному трактується на виходах дешифратора як поточний коефіцієнт розширення. При цьому на всі інші входи надходить сигнал "0", та вони блокуються.

Блоки 5 матричного перетворення обчислюють поточну суму часткових добутоків та приведення її по модулю утворюючого поліному $g^m(x)$. Обчислення поточної суми $\overline{a(x)} * b_1 \oplus \overline{P_{n-1}(x)}$, де

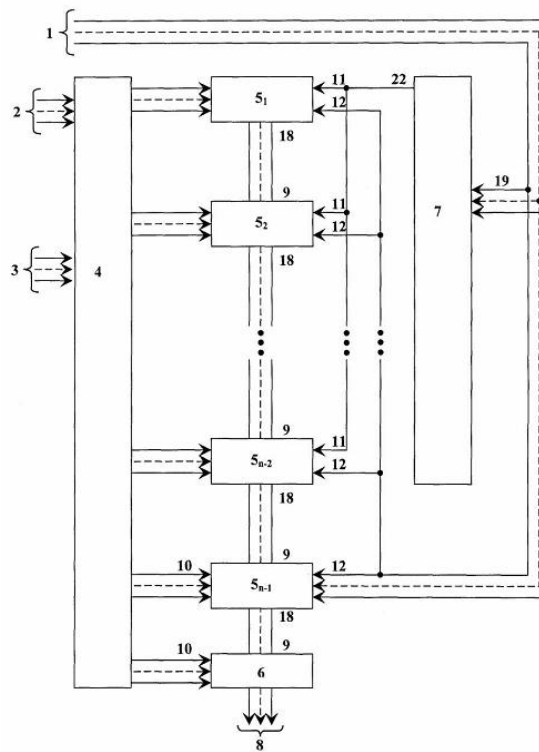
$\overline{a(x)}$ коефіцієнти першого співмножника, b_i - i -тий коефіцієнт другого співмножника, який відповідає номеру i -го поточного блоку 5 матричного перетворення, $\overline{P_{n-1}(x)}$ - коефіцієнти поточної суми $(i-1)$ -го попереднього блоку 5 матричного перетворення, \oplus сума по модулю два, яка виконується першою групою суматорів 13 по модулю два. Приведення по модулю два утворюючого поліному $g^m(x)$ виконується за умови якщо, сума по модулю два $a_k * b_1 \oplus \overline{P_{(i-1)}} = 1/a_k$ та $\overline{P_{(i-1)}}$ відповідно k -ті коефіцієнти першого співмножника та поточної суми попереднього блоку 5 матричного перетворення співпадає зі значенням коефіцієнта розширення поля ("1"), то з суми $\overline{a(x)} * b_i \oplus \overline{P_{n-1}(x)}$ вираховується значення коефіцієнтів $g^m(x)$ утворюючого поліному, що являється результуючою поточною сумою цього блоку. Якщо немає співпадання $a_k * b_1 \oplus \overline{P_{(i-1)}}$ зі значенням коефіцієнта розширення ("0"), то віднімання не виконується, та сума $\overline{a(x)} * b_i \oplus \overline{P_{n-1}(x)}$ передається на вихід блоку. Перша група елементів I 14 застосовується для порівняння коефіцієнта розширення зі знаком $a_k * b_1 \oplus \overline{P_{(i-1)}}$, а друга 16 - для управління відніманням, а $(n-3)$ - входовий елемент АБО 15 призначений для мультиплексування коефіцієнтів розширення. Блок 6 сумування, який складається з $(n-1)$ суматорів по модулю два, призначений для формування коефіцієнтів результуючого добутку, які визначаються як сума $\overline{a(x)} * b_i \oplus \overline{P_{n-1}(x)}$. Множення елементів скінчених полів $GF(2^n)$ виконується як множення многочленів та призводить до обчислення суми часткових добутоків s з приведенням їх по модулю утворюючого поліному.

Таким чином, ефективність запропонованого пристрою визначається його багатифункціональними можливостями (діапазон степені розширення поля), регулярністю структури та можливістю реалізації у вигляді ВІС або ПЛІС.

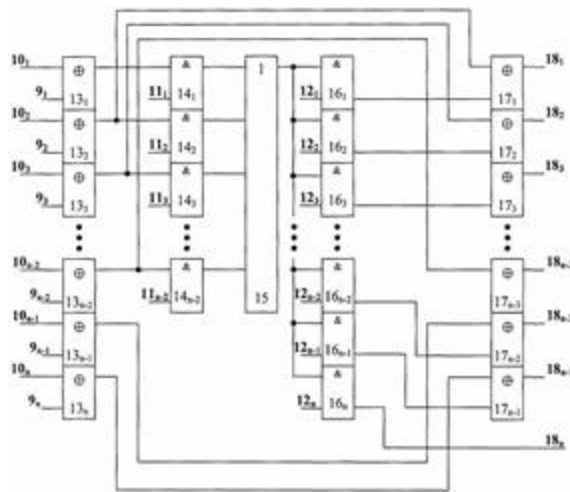
Джерела інформації

1. Патент Російської Федерації №2058040, кл. G06F7/49, 1996.

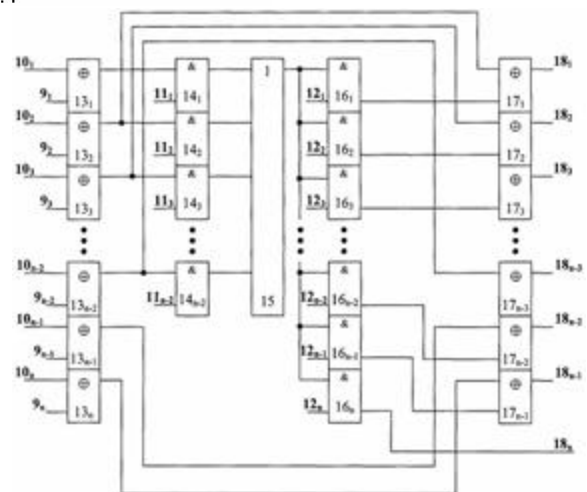
2. Патент України № 4046, кл. G06F7/49, 1994.



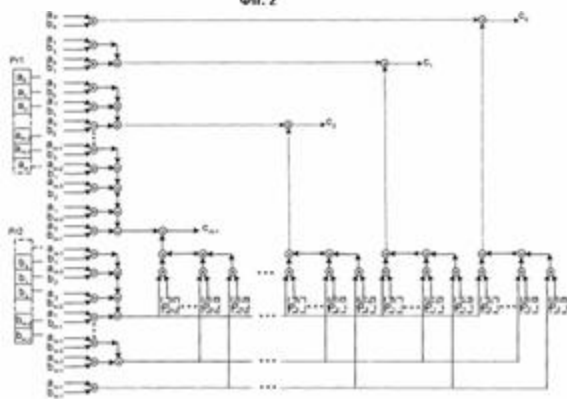
Фиг. 1



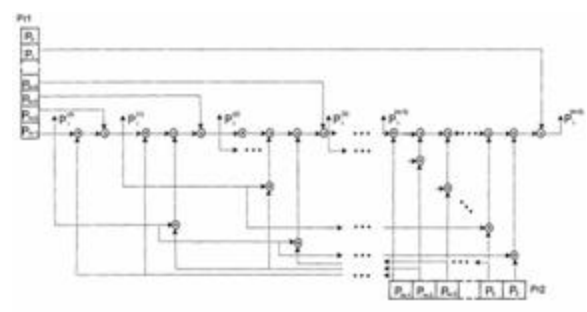
Фиг. 2



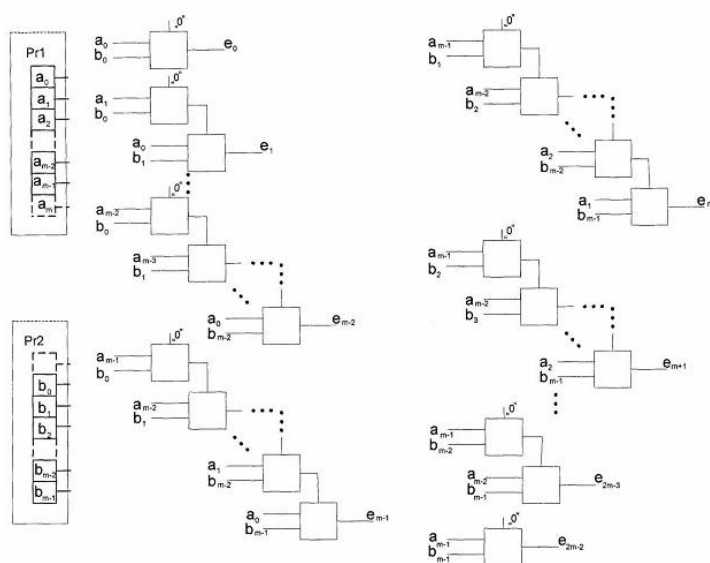
Фиг. 3



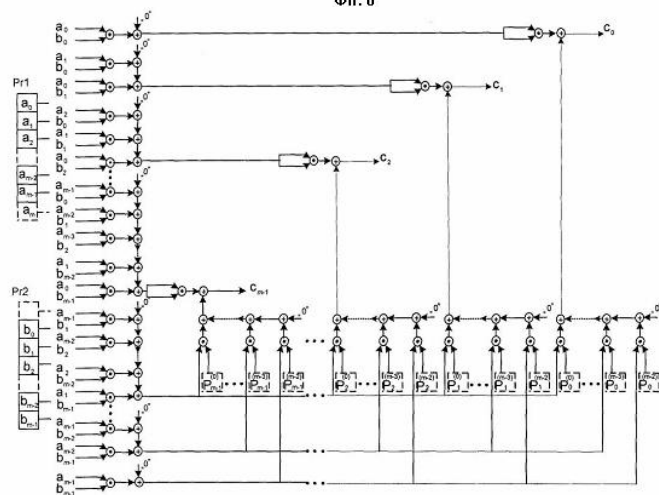
Фиг. 4



Фиг. 5



Фиг. 6



Фиг. 7