



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **103490** (13) **U**
(51) МПК (2015.01)
H03M 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

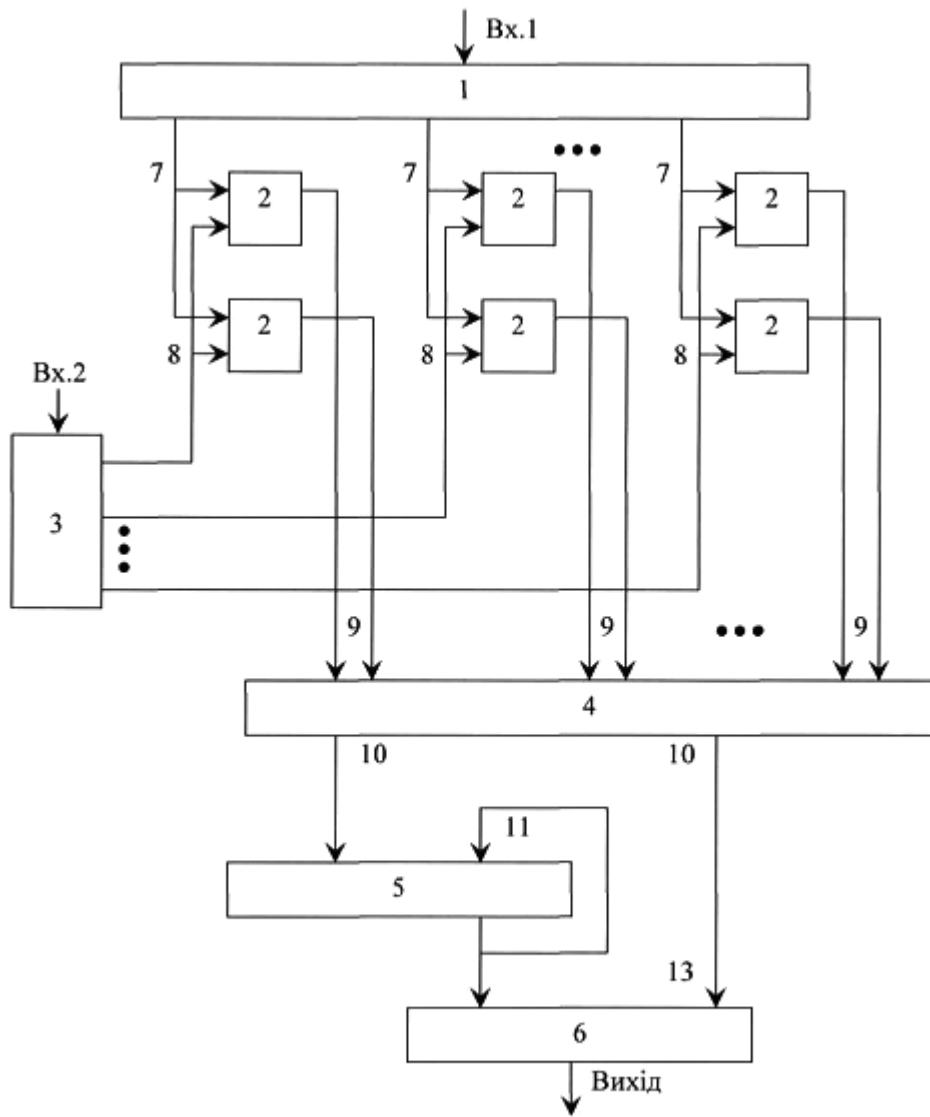
| | |
|--|---|
| (21) Номер заявки: u 2015 01421 | (72) Винахідник(и): Жуков Ігор Анатолійович (UA), Кубицький Валерій Іванович (UA), Синельников Олексій Олексійович (UA) |
| (22) Дата подання заявки: 19.02.2015 | |
| (24) Дата, з якої є чинними права на корисну модель: 25.12.2015 | (73) Власник(и): НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ, пр. Комарова, 1, м. Київ, 03680 (UA) |
| (46) Публікація відомостей про видачу патенту: 25.12.2015, Бюл.№ 24 | |

(54) ПРИСТРІЙ ДЛЯ МНОЖЕННЯ ЕЛЕМЕНТІВ СКІНЧЕННОГО ПОЛЯ GF(2^m) НА КОМБІНАЦІЙНИХ СХЕМАХ

(57) Реферат:

Пристрій для множення елементів скінченного поля GF(2^m) на комбінаційних схемах містить два регістри співмножників, входи яких є входами першого і другого співмножників пристрою, багатовходові суматори за модулем два, виходи яких є елементами I, що об'єднані в групи елементів I, перші входи яких в кожній групі об'єднані і підключені до відповідного виходу регістра першого співмножника, виходи регістра другого співмножника з'єднані з другими входами відповідних елементів I першої групи. В пристрій введено блок обчислення добутку і блок об'єднання загальних доданків, а також пристрій реалізовано на основі комбінаційних схем з використанням функціональних елементів схем I з двома входами, елементів АБО з двома входами та елементів НІ, причому виходи груп елементів I з'єднані з входами блока обчислення компонент множення, виходи якого підключені до входу блока обчислення добутку і входів блока об'єднання загальних доданків, а виходи блока обчислення добутку з'єднані з іншими входами блока об'єднання загальних доданків.

UA 103490 U



Фіг. 1

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 множення елементів скінченних полів, що містить два реєстри співмножників, входи яких є входами першого і другого співмножників пристрою, багатовходові суматори за модулем два, виходи яких є виходами пристрою, елементи I , об'єднані в групи елементів I , перші входи яких в кожній групі об'єднані і підключені до відповідного виходу реєстра першого співмножника, виходи реєстра другого співмножника з'єднані з другими входами відповідних елементів I першої групи, причому виходи реєстра другого співмножника з'єднані з другими входами відповідних елементів I всіх груп елементів I , починаючи з другої групи, виходи груп елементів I з'єднані з входами блока обчислення компонент множення, виходи якого підключені до входів багатовходових суматорів за модулем два і входів блока об'єднання загальних доданків, виходи якого з'єднані з іншими входами багатовходових суматорів за модулем два і входом блока об'єднання загальних доданків [1].

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

Найбільш близьким аналогом є [2] пристрій 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 $(l=1, \dots, n)$ співмножника якого з'єднаний з згрупованими першими входами елементів I i -ої групи блока формування часткових добутків, 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, 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 блока множення 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 блока матричного перетворення $(k=1, \dots, n-2)$, виходи поточної суми $(n-1)$ -го блока матричного перетворення з'єднані з першими входами блока додавання, другі входи якого з'єднані з виходами відповідних елементів I , з першої по $(n-1)$ 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 блока формування часткових добутків, при цьому в кожному блоці матричного перетворення перші входи суматорів по модулю два першої групи з'єднані з входами поточної суми блока, 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 виходами з першого по $(n-1)$ -ий елемент I другої групи, виходи суматорів по модулю два та вихід $(n-2)$ -го елемента I 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 I 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 I другої групи, другі входи яких з'єднані з відповідними входами коефіцієнтів утворюючого поліному блока.

Недоліком даного пристрою є обмеженість функціональних можливостей за рахунок важких апаратних витрат при виконанні операції виявлення та декодування помилок, за рахунок чого зростають часові витрати при кодуванні та декодуванні інформації.

В основу корисної моделі поставлена задача удосконалення пристрою для множення елементів скінченних полів $GF(2^n)$ шляхом зменшення параметрів часу обчислення та шляхом реалізації пристрою на комбінаційних схемах.

Це дозволяє забезпечити безпосереднє виконання операції множення елементів скінченних полів $GF(2^m)$ методами, що використовують логічні функції, тобто має широкі функціональні можливості застосування їх в процедурах кодування та декодування кодів.

Поставлена задача вирішується тим, що в пристрої множення елементів скінченного поля (2^m) , що містить два реєстри співмножників, входи яких є входами першого і другого співмножників пристрою, багатовходові суматори за модулем два, виходи яких є елементами I , що об'єднані в групи елементів I , перші входи яких в кожній групі об'єднані і підключені до відповідного виходу реєстра першого співмножника, виходи реєстра другого співмножника з'єднані з другими входами відповідних елементів I першої групи, а також, згідно з корисною моделлю, в пристрій введено блок обчислення добутку і блок об'єднання загальних доданків, а

також пристрій реалізовано на основі комбінаційних схем з використанням функціональних елементів схем І з двома входами, елементів АБО з двома входами та елементів НІ, причому виходи груп елементів І з'єднані з входами блока обчислення компонент множення, виходи якого підключені до входу блока обчислення добутку і входів блока об'єднання загальних доданків, а виходи блока обчислення добутку з'єднані з іншими входами блока об'єднання загальних доданків.

Множення елементів скінченного поля, наприклад із застосуванням комбінаційної схеми множення, що реалізує алгоритм множення у відповідності з виразом $(A_1 \oplus P \otimes A_2^*) \otimes B = A \otimes B$, має 1-ий рівень, на якому обчислюється матриця, що складається з наступних груп функціональних осередків

$$\begin{aligned} G_1^{(1)} &= \{D_{11}^{(1)}, D_{12}^{(1)}, \dots, D_{1,m-1}^{(1)}\} \\ G_2^{(1)} &= \{D_{21}^{(1)}, D_{22}^{(1)}, \dots, D_{2,m-1}^{(1)}\} \\ &\vdots \\ G_m^{(1)} &= \{D_{m1}^{(1)}, D_{m2}^{(1)}, \dots, D_{m,m-1}^{(1)}\} \end{aligned}$$

де $D_{ij}^{(1)}$ - блоки, що складаються з схем І та суматорів по модулю 2. Цей рівень містить $m^2(m-1)/2$ схем І та $m(m-1)^2/2$ суматорів по модулю 2. Наявність схем І дає можливість змінювати багаточлен $p(x)$. При фіксованому багаточлені $p(x)$ ці схеми не потрібні, оскільки значення $p_i^{(i)}$ містяться в структурі 1-го рівня.

На другому рівні виконується множення матриць $D_2 \otimes B$, що містить m^1 схем І та $m(m-1)$ суматорів по модулю 2.

Комбінаційна схема множення для варіанта побудови з можливістю зміни багаточлена $p(x)$ та зберігання значень $p_i^{(i)}$ представлена на кресленні 2.

Універсальна комбінаційна схема, що реалізує вираз $(A_1 \oplus P \otimes A_2^*) \otimes B = A \otimes B$ побудована на основі функціональних осередків, має також два рівня та представлена на кресленні 3.

1-й рівень комбінаційної схеми складають блоки функціональних осередків $D_{ij}^{(1)}$ ($i = \overline{1, m}, j = \overline{1, m-1}$), кожний з яких складається з одного $(D_{11}^{(1)}, D_{21}^{(1)}, \dots, D_{m1}^{(1)})$ або декількох блоків.

2-й рівень складається з функціональних осередків C_i ($i = \overline{0, m-1}$), кожний з яких містить m блоків.

Із застосуванням алгоритму при визначенні контрольних символів потрібно в 2 рази менше операцій модульного множення.

В результаті це дозволяє забезпечити безпосередньо виконувати операції декодування одиночних недвійкових помилок, і як наслідок, розширення функціональних можливостей побудови комбінаційних схем.

На кресленні фіг. 1 зображена структурна схема пристрою множення елементів скінченних полів $GF(2^m)$ на комбінаційних схемах. На кресленні фіг. 2 - приклад схеми пристрою множення елементів скінченних полів $GF(2^m)$ на комбінаційній схемі з можливістю зміни багаточлена $p(x)$ та зберігання значень $p_i^{(i)}$. На кресленні 3 - приклад схеми пристрою множення елементів скінченних полів $GF(2^m)$ на універсальній комбінаційній схемі.

Пристрій для множення елементів скінченних полів $GF(2^m)$ на комбінаційних схемах містить два регістри співмножників, входи яких є входами першого і другого співмножників пристрою $Vx.1$ та $Vx.2$, багатовходові суматори за модулем два 1 та 3, виходи яких є елементами І 2, що об'єднані в групи елементів І 2, перші входи 7 яких в кожній групі об'єднані і підключені до відповідного виходу регістра першого співмножника, виходи регістра другого співмножника 8 з'єднані з другими входами відповідних елементів І першої групи, а також, згідно з корисною моделлю, в пристрій введено блок обчислення добутку 5 і блок об'єднання загальних доданків 6, а також пристрій реалізовано на основі комбінаційних схем з використанням функціональних елементів схем І з двома входами елементів АБО з двома входами та елементів НІ, причому виходи груп елементів І 9 з'єднані з входами блока обчислення компонент множення 4, виходи якого 10 підключені до входу блока обчислення добутку 5 і входів 13 блока об'єднання загальних доданків 6, а виходи блока обчислення добутку 5 з'єднані з іншими входами 11 блока об'єднання загальних доданків 6.

Пристрій для множення елементів скінченного поля $GF(2^m)$ на комбінаційних схемах працює в такий спосіб.

Перед початком множення значення потрапляють на входи співмножників пристрою Вх.1 та Вх.2, що являють собою багатовходові суматори за модулем два 1 та 3, результати яких надходять на виходи цих елементів І 2, що об'єднані в групи елементів І 2. Здійснюється множення матриць $P \otimes A_2^*$, результати яких потрапляють на входи 7, які в кожній групі об'єднані і підключені до відповідного виходу регістра першого співмножника, виходи регістра другого співмножника 8 з'єднані з другими входами відповідних елементів І першої групи, причому виходи груп елементів І 9 з'єднані з входами блока обчислення компонент множення 4, де виконується додавання матриць $A_1 \oplus D_1$, виходи якого 10 підключені до входу блока обчислення добутку 5 і входів 13 блока об'єднання загальних доданків 6, а виходи блока обчислення добутку 5 з'єднані з іншими входами 11 блока об'єднання загальних доданків 6. Остаточні результати множення матриць $D_2 \otimes B$ надходять на вихід пристрою.

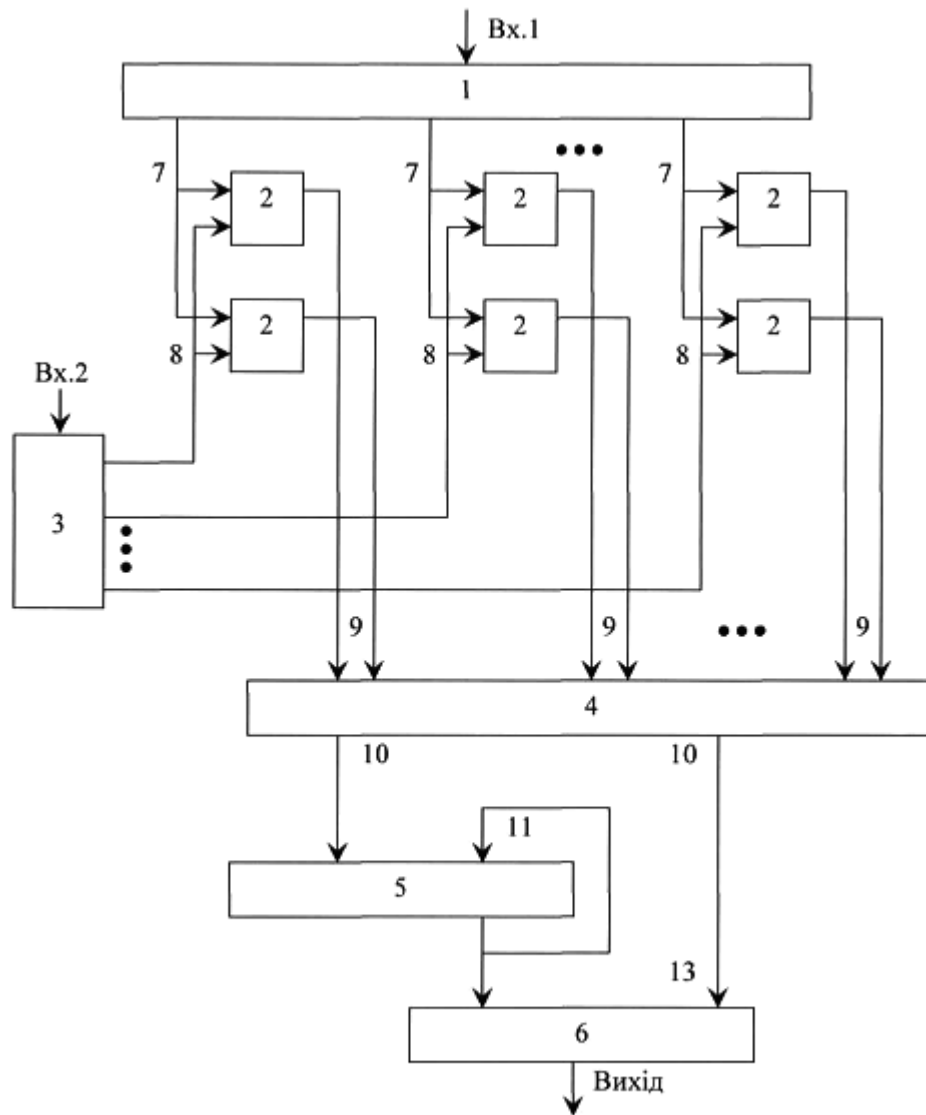
Таким чином, ефективність запропонованого пристрою визначається його багатofункціональними можливостями (запропоновано метод множення елементів скінченного поля, що базується на використанні логічних функцій), регулярністю структури та можливістю реалізації у вигляді ВІС або ПЛІС.

Джерела інформації:

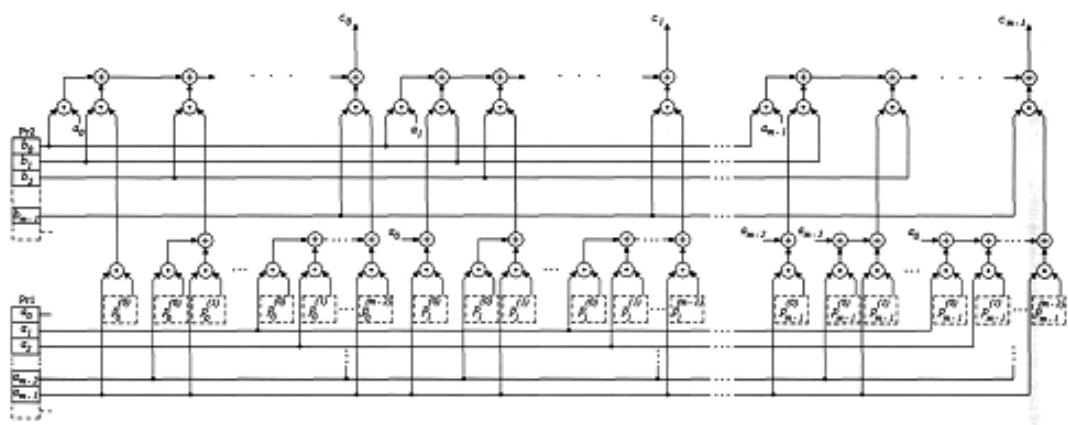
1. Патент Російської Федерації № 35930, кл. H03M 13/05, 2004
2. Деклараційний патент на корисну модель № 43629, кл. H03M 7/00, 2009.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

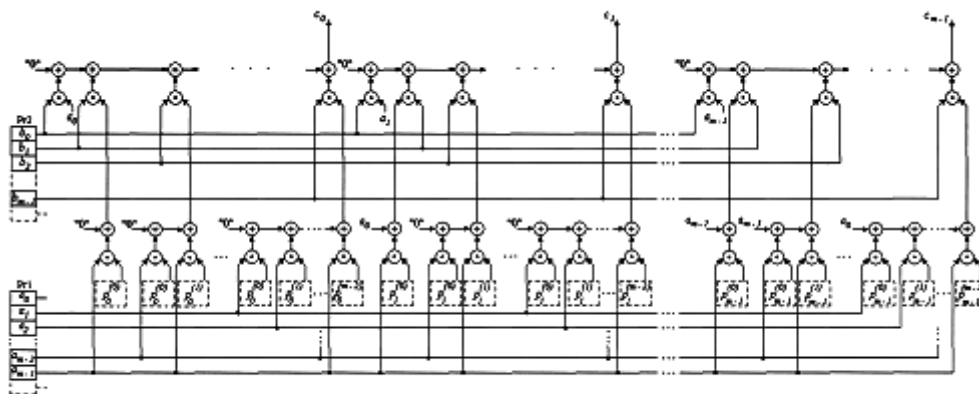
Пристрій для множення елементів скінченного поля $GF(2^m)$ на комбінаційних схемах, що містить два регістри співмножників, входи яких є входами першого і другого співмножників пристрою, багатовходові суматори за модулем два, виходи яких є елементами І, що об'єднані в групи елементів І, перші входи яких в кожній групі об'єднані і підключені до відповідного виходу регістра першого співмножника, виходи регістра другого співмножника з'єднані з другими входами відповідних елементів І першої групи, який **відрізняється** тим, що в пристрій введено блок обчислення добутку і блок об'єднання загальних доданків, а також пристрій реалізовано на основі комбінаційних схем з використанням функціональних елементів схем І з двома входами, елементів АБО з двома входами та елементів НІ, причому виходи груп елементів І з'єднані з входами блока обчислення компонент множення, виходи якого підключені до входу блока обчислення добутку і входів блока об'єднання загальних доданків, а виходи блока обчислення добутку з'єднані з іншими входами блока об'єднання загальних доданків.



Фіг. 1



Фіг. 2



Фиг. 3