



УКРАЇНА

(19) UA (11) 33447 (13) U
(51) МПК (2006)
G06F 5/00
G06F 17/14

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) ПРИСТРІЙ ДЛЯ ОБЧИСЛЕННЯ ДВОТОЧКОВОГО ЗРІЗАНОГО ПЕРЕТВОРЕННЯ ФУР'Є В ПОЛІ $GF(2^{16})$

1

(21) u200801389

(22) 04.02.2008

(46) 25.06.2008, Бюл.№ 12, 2008 р.

(72) РУБАН ІГОР ВІКТОРОВИЧ, UA, ДУДЕНКО СЕРГІЙ ВАСИЛЬОВИЧ, UA, АЛЕКСЄЄВ СЕРГІЙ ВІКТОРОВИЧ, UA, СІОРА ОЛЕКСАНДР АНДРІЙОВИЧ, UA, ХЕРІ АЛІ АБДУЛЛАХ, UA, КОШМАН СЕРГІЙ ОЛЕКСАНДРОВИЧ, UA, КРАСНОБАЄВ ВІКТОР АНАТОЛІЙОВИЧ, UA

(73) РУБАН ІГОР ВІКТОРОВИЧ, UA, ДУДЕНКО СЕРГІЙ ВАСИЛЬОВИЧ, UA, АЛЕКСЄЄВ СЕРГІЙ ВІКТОРОВИЧ, UA, СІОРА ОЛЕКСАНДР АНДРІЙОВИЧ, UA, ХЕРІ АЛІ АБДУЛЛАХ, UA, КОШМАН СЕРГІЙ ОЛЕКСАНДРОВИЧ, UA, КРАСНОБАЄВ ВІКТОР АНАТОЛІЙОВИЧ, UA

(57) Пристрій для обчислення двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$, який містить блок оперативної пам'яті, перший та другий блоки постійної пам'яті, перший та другий мультиплексори, блок складання по модулю два, перший, другий та третій регістри, блок керування, до складу якого входять генератор тактових імпульсів, перший, другий та третій тригери, перший, другий та третій лічильники, дешифратор, перший, другий та третій елементи І, формувач фронтів, перший та другий елементи АБО, D-тригер, постійний запам'ятовуючий пристрій, який **відрізняється** тим, що змінено розрядність (з восьми на шістнадцять розрядів) блока оперативної пам'яті, першого та другого блоків постійної пам'яті, першого та другого мультиплексорів, блока складання по модулю два, першого, другого та третього регістрів, при цьому вхід запуску пристрою з'єднаний з входом блока керування, адресний вхід блока оперативної пам'яті з'єднаний з першим виходом блока керування, вхід дозволу читання блока оперативної пам'яті з'єднаний з другим виходом блока керування, вихід блока оперативної пам'яті з'єднаний з адресними входами першого та другого блоків постійної пам'яті, входи дозволу читання першого та другого блоків постійної пам'яті з'єднані з другим виходом блока керування, вихід першого блока постійної пам'яті з'єднаний з першим входом першого мультиплексора, вихід другого блока постійної пам'яті з'єднаний з другим входом першого мультиплексора, адресний вхід першого мульти-

2

плексора з'єднаний з третім виходом блока керування, вихід першого мультиплексора з'єднаний з другим входом блока, що реалізує операцію складання по модулю два, вихід блока, що реалізує операцію складання по модулю два, з'єднаний з входами даних першого та другого регістрів, вихід дозволу запису першого та другого регістрів з'єднані з четвертим виходом блока керування, вихід першого регістра з'єднаний з першим входом другого мультиплексора, вихід другого регістра з'єднаний з другим входом другого мультиплексора, адресний вхід другого мультиплексора з'єднаний з п'ятим виходом блока керування, вихід другого мультиплексора з'єднаний з входом даних третього регістра, вхід дозволу запису третього регістра з'єднаний з п'ятим виходом блока керування, вихід третього регістра є виходом пристрою та з'єднаний з першим входом блока, що реалізує операцію складання по модулю два, вхід блока керування з'єднаний з входом переводу першого тригера в одиницю, вихід першого тригера з'єднаний з входом генератора тактових імпульсів, вихід якого з'єднаний з рахунковим входом другого лічильника та другими входами другого та третього елементів І, вхід скидання першого тригера з'єднаний з виходом переповнення (переносу) першого лічильника, перший вихід другого лічильника (молодший розряд) з'єднаний з першим входом дешифратора (молодший розряд) і першим входом першого елемента І, другий вихід другого лічильника з'єднаний з другим входом дешифратора, третій вихід другого лічильника (старший розряд) з'єднаний з третім входом дешифратора (старший розряд) і другим входом першого елемента І, вихід першого елемента І з'єднаний з входом формувача фронтів, вихід формувача фронтів з'єднаний з входом першого лічильника, входом обнуління другого лічильника, входами обнуління другого та третього тригерів, перший вихід дешифратора з'єднаний з входом переводу другого тригера в одиницю, другий вихід дешифратора з'єднаний з входом переводу третього тригера в одиницю, третій вихід дешифратора з'єднаний з першим входом першого елемента АБО, четвертий вихід дешифратора з'єднаний з першим входом другого елемента АБО і першим входом другого елемента І, п'ятий вихід

U
(13)

33447
(11)

UA
(19)

дешифратора з'єднаний з другим входом першого елемента АБО, шостий вихід дешифратора з'єднаний з другим входом другого елемента АБО і першим входом третього елемента І, вихід першого елемента АБО з'єднаний з входом D-тригера, вихід другого елемента АБО з'єднаний з тактовим входом третього лічильника, виходи третього лічильника з'єднані з входами постійного запам'ятовуючого пристрою, вихід першого лічильника по першому виходу блока керування з'єднаний з адресним входом блока оперативної пам'яті, вихід другого тригера по другому виходу блока керування з'єднаний з входом дозволу читання блока оперативної пам'яті, вихід третього тригера по другому виходу блока керування з'єднаний з входами

дозволу читання першого та другого блоків постійної пам'яті, вихід постійного запам'ятовуючого пристрою по третьому виходу блока керування з'єднаний з адресним входом першого мультиплексора, вихід другого елемента І по четвертому виходу блока керування з'єднаний з входом дозволу запису першого регістра, вихід третього елемента І по четвертому виходу блока керування з'єднаний з входом дозволу запису другого регістра, вихід першого елемента АБО по п'ятому виходу блока керування з'єднаний з входом дозволу запису третього регістра, вихід D-тригера по п'ятому виходу блока керування з'єднаний з адресним входом другого мультиплексора.

Запропонована корисна модель відноситься до галузі автоматики й обчислювальної техніки і може бути використана в системах кодування даних.

Відомий "Пристрій для швидкого дійсного перетворення Хартлі-Фур'є", що містить блок синхронізації, два лічильника адреси, блок постійної пам'яті, вхідний регістр, регістр, вихідний регістр, блок пам'яті, два перемножувача, два комутатора, суматор-вчитач, вихідний регістр, комутатор, інформаційний вхід, інформаційний вихід [а.с. 1569847 СРСР №4473106, МКИ G06F15/332, 1988, Бюл. №21, 1990р.].

Недоліком пристрою є те, що він не виконує обчислень векторів.

Відомий також "Пристрій для обчислення усередненого перетворення Фур'є в остаточних класах", який містить блок оперативної пам'яті, перший, другий, третій та четвертий блоки постійної пам'яті, перший, другий та третій блоки, які реалізують операцію складання по модулю два, перший, другий, третій та четвертий допоміжні блоки постійної пам'яті, перший, другий, третій та четвертий регістри, блок управління, до складу якого входять генератор тактових імпульсів, тригер, лічильник, дешифратор, перший, другий, третій та четвертий елементи І [Деклараційний патент №4264 У України №2004032321, 7МПК G06F7/04, 2004, Бюл. №1 2005р.].

Недоліком пристрою є те, що він обчислює зрізане перетворення Фур'є в залишкових класах табличним способом.

Найбільш близьким за технічною суттю і результатом, що досягається, є "Пристрій для обчислення двоточкового зрізаного перетворення Фур'є в полі $GF(2^8)$ " [Деклараційний патент на корисну модель №23421 У України №u200613776, МПК(2006) G06F5/00, G06F17/14, 2006, Бюл. №7 2007р.], який містить блок оперативної пам'яті, перший та другий блоки постійної пам'яті, перший та другий мультиплексори, блок складання по модулю два, перший, другий та третій регістри, блок керування, до складу якого входять генератор тактових імпульсів, перший, другий та третій тригери, перший, другий та третій лічильники, дешифратор,

перший, другий та третій елементи І, формувач фронтів, перший та другий елементи АБО, D-тригер, постійний запам'ятовуючий пристрій.

Недоліком пристрою відомого пристрою є низькі функціональні можливості, які полягають в тому, що він обчислює математичним способом двоточкове зрізане перетворення Фур'є в полі $GF(2^8)$.

В основу корисної моделі поставлено задачу - розширити функціональні можливості за рахунок вдосконалення пристрою для обчислення двоточкового зрізаного перетворення Фур'є в полі $GF(2^8)$, який зможе реалізувати знаходження вихідного вектора для двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$ математичним способом.

Зрізане перетворення Фур'є в залишкових класах визначено [4]:

$$V_j = \sum_{i=1}^{n-1} W^{ij} \cdot v_i, (1)$$

$$v_i = \left(\frac{1}{n \bmod p} \right) \sum_{j=1}^{n-1} (W^{-ij} \oplus L) \cdot V_j, (2)$$

де w - елемент порядку p у полі $GF(q^m)$;

i - номер точки вхідного вектору (для двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$ $i=1,2$);

j - номер точки вихідного вектору (для двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$ $j=1,2$);

$\oplus$ - операція складання у полі;

$L = -1$.

Існує два способи знаходження вихідного вектора:

1. Математичний спосіб, який полягає у виконанні всіх математичних операцій згідно (1).

2. Табличний спосіб, який полягає в тому, що створюють $(n-1)$ таблиць, які складаються з 2^m елементів, розміру $m-(n-1)$ біт, а вихідний вектор отримують шляхом складання елементів таблиць, які відповідають точкам вхідного вектору.

Поставлена задача вирішується за рахунок того, що у пристрої-прототипі змінено розрядність (з восьми на шістнадцять розрядів) блоку оперативної пам'яті, першого та другого блоків постійної

пам'яті, першого та другого мультиплексорів, блоку складання по модулю два, першого, другого та третього регістрів. Також додатково введені нові зв'язки увсьому пристрої.

Технічний результат, який може бути отриманий при використанні корисної моделі, полягає в одержанні технічного засобу для знаходження вихідного вектора при реалізації двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$ математичним способом.

На Фіг.1 приведена блок-схема запропонованого пристрою.

На Фіг.2 приведена блок-схема блока керування запропонованого пристрою.

Запропонований пристрій для обчислення двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$ містить блок оперативної пам'яті 1, перший та другий блоки постійної пам'яті 2 і 3, блок керування 4, перший мультиплексор 5, блок складання по модулю два 6, перший та другий регістри 7 і 8, другий мультиплексор 9, третій регістр 10, вхід запуску 11, вихід 12, причому вхід запуску 11 пристрою з'єднаний з входом блока керування. Адресний вхід блока оперативної пам'яті 1 з'єднаний з виходом 13 блока керування. Вхід дозволу читання блока оперативної пам'яті 1 з'єднаний з виходом 14 блока керування. Вихід блока оперативної пам'яті 1 з'єднаний з адресними входами блоків постійної пам'яті 2 і 3. Входи дозволу читання блоків постійної пам'яті 2 і 3 з'єднані з виходом 14 блока керування. Вихід блока постійної пам'яті 2 з'єднаний з першим входом мультиплексора 5. Вихід блока постійної пам'яті 3 з'єднаний з другим входом мультиплексора 5. Адресний вхід мультиплексора 5 з'єднаний з виходом 15 блока керування. Вихід мультиплексора 5 з'єднаний з другим входом блока 6, що реалізує операцію складання по модулю два. Вихід блока 6, що реалізує операцію складання по модулю два, з'єднаний з входами даних регістрів 7 і 8. Входи дозволу запису регістрів 7 і 8 з'єднані з виходом 16 блока керування. Вихід регістра 7 з'єднаний з першим входом мультиплексора 9. Вихід регістра 8 з'єднаний з другим входом мультиплексора 9. Адресний вхід мультиплексора 9 з'єднаний з виходом 17 блока керування. Вихід мультиплексора 9 з'єднаний з входом даних регістра 10. Вхід дозволу запису регістра 10 з'єднаний з виходом 17 блока керування. Вихід регістра 10 є виходом 12 пристрою та з'єднаний з першим входом блока 6, що реалізує операцію складання по модулю два.

Блок керування 4 пристрою для обчислення двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$ містить: генератор тактових імпульсів 18, перший тригер 19, перший та другий лічильники 20 і 21, дешифратор 22, перший елемент І 23, формувач фронтів 24, перший та другий елементи АБО 25 і 26, D-тригер 27, третій лічильник 28, другий та третій тригери 29 і 30, постійний запам'ятовуючий пристрій 31, другий та третій елементи І 32 і 33, причому вхід 11 блока керування з'єднаний з входом переводу тригера 19 в одиницю, вихід тригера 19 з'єднаний з входом генератора тактових імпульсів 18, вихід якого з'єднаний з рахунковим входом лічильника 21 та другими вхо-

дами елементів І 32 і 33. Вхід скидання тригера 19 з'єднаний з виходом переповнення (переносу) лічильника 20. Перший вихід лічильника 21 (молодший розряд) з'єднаний з першим входом дешифратора 22 (молодший розряд) і першим входом елемента І 23. Другий вихід лічильника 21 з'єднаний з другим входом дешифратора 22. Третій вихід лічильника 21 (старший розряд) з'єднаний з третім входом дешифратора 22 (старший розряд) і другим входом елемента І 23. Вихід елемента І 23 з'єднаний з входом формувача фронтів 24. Вихід формувача фронтів 24 з'єднаний з входом лічильника 20, входом обнуління лічильника 21, входами обнуління тригерів 29 і 30. Перший вихід дешифратора 22 з'єднаний з входом переводу тригера 29 в одиницю, другий вихід дешифратора 22 з'єднаний з входом переводу тригера 30 в одиницю, третій вихід дешифратора 22 з'єднаний з першим входом елемента АБО 25, четвертий вихід дешифратора 22 з'єднаний з першим входом елемента АБО 26 і першим входом елемента І 32, п'ятий вихід дешифратора 22 з'єднаний з другим входом елемента АБО 25, шостий вихід дешифратора 22 з'єднаний з другим входом елемента АБО 26 і першим входом елемента І 33. Вихід елемента АБО 25 з'єднаний з входом D-тригера 27. Вихід елемента АБО 26 з'єднаний з тактовим входом лічильника 28. Вихід лічильника 28 з'єднаний з входами постійного запам'ятовуючого пристрою 31. Вихід лічильника 20 по виходу 13 блока керування 4 з'єднаний з адресним входом блока оперативної пам'яті 1. Вихід тригера 29 по виходу 14 блока керування 4 з'єднаний з входом дозволу читання блока оперативної пам'яті 1. Вихід тригера 30 по виходу 14 блока керування 4 з'єднаний з входами дозволу читання блоків постійної пам'яті 2 і 3. Вихід постійного запам'ятовуючого пристрою 31 по виходу 15 блока керування 4 з'єднаний з адресним входом мультиплексора 5. Вихід елемента І 32 по виходу 16 блока керування 4 з'єднаний з входом дозволу запису регістра 7. Вихід елемента І 33 по виходу 16 блока керування 4 з'єднаний з входом дозволу запису регістра 8. Вихід елемента АБО 25 по виходу 17 блока керування 4 з'єднаний з входом дозволу запису регістра 10. Вихід D-тригера 27 по виходу 17 блока керування 4 з'єднаний з адресним входом мультиплексора 9.

Робота запропонованого пристрою здійснюється за два цикли по шість тактів у кожному та полягає в наступному. Перед початком роботи в блок оперативної пам'яті 1 записаний вхідний вектор $v = \{v_1, v_2\}$ в двійковому коді, причому $v_1 \in GF(2^{16})$.

В блоки постійної пам'яті 2 і 3 за адресою $v_i = 0 \div 65535$ записані результати множення в полі $GF(2^{16})$ у виді

$$\{P(v_i w^j)\},$$

де $P(X)$ - перехід від десяткового представлення елемента поля $GF(2^{16})$ до двійкового представлення;

w - елемент порядку p у полі $GF(q^m)$;

i - номер точки вхідного вектору;

j - номер точки вихідного вектору.

Регістри 7, 8 і 10, тригер 19, лічильники 20 і 21, D-тригер 27, лічильник 28, тригери 29 і 30 у нульовому стані.

На виході дешифратора 22 під час роботи пристрою формується унітарний код такту, причому рівень "1" буде тільки на одному з його виходів.

Постійний запам'ятовуючий пристрій 31 містить для кожного з тактів 4 і 6 циклів 1 і 2 адреси, що використовують для адресації мультиплексора 5 з метою здійснення математичного способу знаходження вихідного вектора при реалізації двоточкового зрізаного перетворення Фур'є в полі $GF(2^{16})$.

По сигналу "Запуск обробки", що надходить по входу 11 пристрою, тригер 19 встановлюється в одиничний стан, сигнал "1" з виходу тригера 19 надходить на вхід генератора тактових імпульсів 18, що починає формувати послідовність тактових імпульсів, що надходять на рахунковий вхід лічильника 21 та другі входи елементів І 32 і 33.

Цикл 1.

На першому такті формується рівень "1" на першому виході дешифратора 22, що встановлює тригер 29 в одиницю. Рівень "1" з виходу тригера 29 через вихід 14 блока керування 4 поступає на вхід дозволу читання блока оперативної пам'яті 1, на виході якого формується двійкове представлення числа v_1 .

На другому такті формується рівень "1" на другому виході дешифратора 22, що встановлює тригер 30 в одиницю. Рівень "1" з виходу тригера 30 через вихід 14 блока керування 4 поступає на входи дозволу читання блоків постійної пам'яті 2 і 3. При цьому на виходах блоків постійної пам'яті 2 і 3 формується двійкове представлення результату множення $v_1 w^{ij}$ у полі $GF(2^{16})$. Двійкове представлення результату множення з виходу відповідного блока постійної пам'яті (2 або 3) через мультиплексор 5 поступає на другий вхід блока 6. З виходу блока 6 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 10, поступає на входи даних регістрів 7 і 8.

На третьому такті формується рівень "1" на третьому виході дешифратора 22, що з виходу елемента АБО 25 через вихід 17 блока керування 4 по передньому фронту імпульсу в регістр 10 через мультиплексор 9 записує значення, що міститься у регістрі 7. По задньому фронту імпульсу з виходу елемента АБО 25 D-тригер 27 встановлюється в одиницю. Рівень "1" з виходу D-тригера 27 через вихід 17 блока керування 4 поступає на адресний вхід мультиплексора 9 та комує на вхід даних регістра 10 вихід регістра 8.

На четвертому такті формується рівень "1" на четвертому виході дешифратора 22, що з виходу елемента І 32 через вихід 16 блока керування 4 записує до регістра 7 результат складання по модулю два результату множення v_1 у полі $GF(2^{16})$ зі значенням, що міститься на виході регістра 10. Рівень "1" з четвертого виходу дешифратора 22 поступає на елемент АБО 26. По передньому

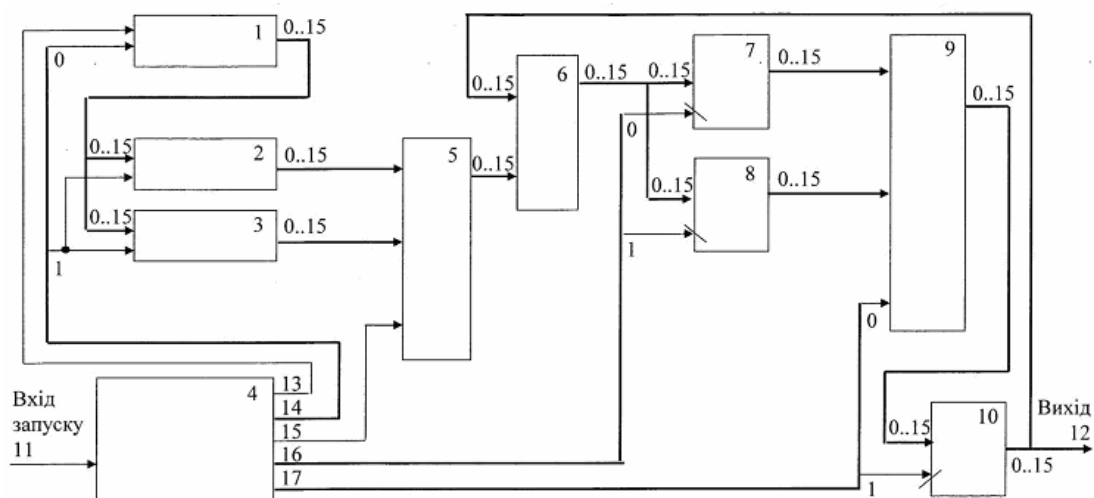
фронту імпульсу з виходу елемента АБО 26 лічильник 28 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 31 через вихід 15 блока керування 4 на адресному вході мультиплексора 5 встановлюється новий адрес і двійкове представлення результату множення v_i у полі $GF(2^{16})$ з виходу відповідного блока постійної пам'яті (2 або 3) через мультиплексор 5 поступає на другий вхід блока 6. З виходу блока 6 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 10, поступає на входи даних регістрів 7 і 8.

На п'ятому такті формується рівень "1" на п'ятому виході дешифратора 22, що з виходу елемента АБО 25 через вихід 17 блока керування 4 по передньому фронту імпульсу в регістр 10 через мультиплексор 9 записує значення, що міститься у регістрі 8. По задньому фронту імпульсу з виходу елемента АБО 25 D-тригер 27 встановлюється в 0. Рівень "0" з виходу D-тригера 27 через вихід 17 блока керування 4 поступає на адресний вхід мультиплексора 9 та комує на вхід даних регістра 10 вихід регістра 7.

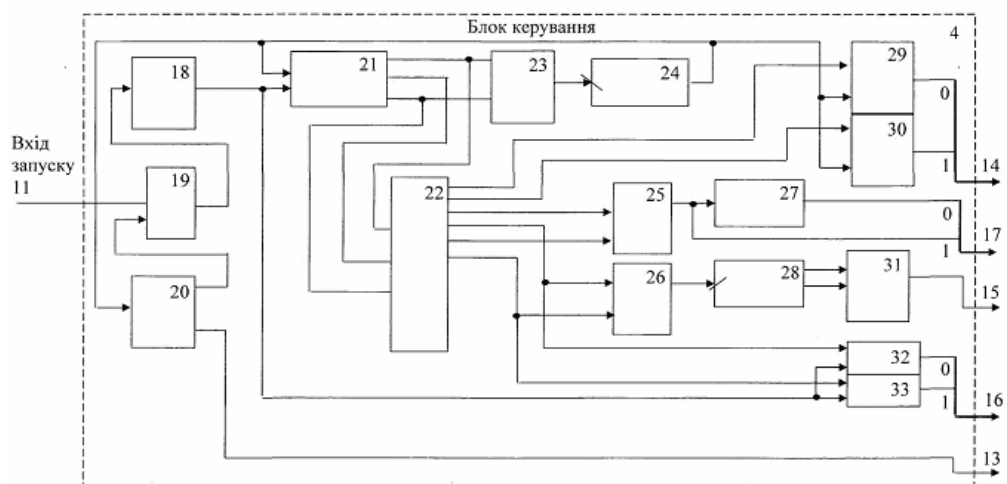
На шостому такті формується рівень "1" на шостому виході дешифратора 22, що з виходу елемента І 33 через вихід 16 блока керування 4 записує до регістра 8 результат складання по модулю два результату множення v_1 у полі $GF(2^{16})$ зі значенням, що міститься на виході регістра 10. Рівень "1" з шостого виходу дешифратора 22 поступає на елемент АБО 26. По передньому фронту імпульсу з виходу елемента АБО 26 лічильник 28 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 31 через вихід 15 блока керування 4 на адресному вході мультиплексора 5 встановлюється новий адрес і двійкове представлення результату множення v_i у полі $GF(2^{16})$ з виходу відповідного блока постійної пам'яті (2 або 3) через мультиплексор 5 поступає на другий вхід блока 6. З виходу блока 6 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 10, поступає на входи даних регістрів 7 і 8. По задньому фронту імпульсу з виходу елемента І 23 через формувач фронтів 24 здійснюється збільшення на одиницю лічильника 20, обнуління лічильника 21 та встановлення в "0" тригерів 29 і 30. Рівень "1" з виходу лічильника 20 через вихід 13 блока керування 4 встановлює на адресному вході блока оперативної пам'яті 1 адресу для зчитування двійкового представлення числа v_2 .

Цикл 2 здійснюється аналогічно циклу 1 за винятком того, що всі операції здійснюються з використанням двійкового представлення числа v_2 .

Після завершення останнього такту другого циклу на виході переповнення лічильника 20 формується рівень "1", що скидає тригер 19 у нульовий стан, а пристрій повертається у початковий стан, при цьому з виходу 12 пристрою через мультиплексор 9 і регістр 10 зчитують остаточний результат, що міститься на виходах регістрів 7 і 8.



Фіг. 1



Фіг. 2