

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" [1], який 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.

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

Відомий також "Пристрій для обчислення усіченого перетворення Фур'є в остаточної клас" [2], 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.

Недоліком пристрою є те, що він обчислює усічене перетворення Фур'є в остаточної клас табличним способом.

Найбільш близьким до запропонованого технічним рішенням, обраним як прототип, є "Пристрій для обчислення усіченого перетворення Фур'є в залишкових клас" [3], який містить блок оперативної пам'яті, перший, другий, третій та четвертий блоки постійної пам'яті, перший та другий мультиплексори, блок складання по модулю два, перший, другий, третій, четвертий та п'ятий регістри, блок керування, до складу якого входять генератор тактових імпульсів, перший, другий та третій тригери, перший, другий, третій та четвертий лічильники, дешифратор, перший, другий, третій, четвертий та п'ятий елементи І, формувач фронтів, перший та другий елементи АБО, постійний запам'ятовуючий пристрій.

Недоліком пристрою-прототипу є те, що він обчислює математичним способом чотирьохточкове усічене перетворення Фур'є в полі $GF(2^8)$.

В основу корисної моделі поставлена задача створити "Пристрій для обчислення 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$ ", який реалізує знаходження вихідного вектора для 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$ математичним способом.

Усічене перетворення Фур'є в залишкових клас визначено [4]:

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

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

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

i - номер точки вхідного вектору (для 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$ $i=1, 2, \dots, 14$);

j - номер точки вихідного вектору (для 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$ $j=1, 2, \dots, 14$);

$\oplus$ - 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 $m \cdot (n-1)$ біт, а вихідний вектор отримують шляхом складання елементів таблиць, які відповідають точкам вхідного вектору.

Поставлена задача вирішується за рахунок того, що у пристрій-прототип додатково введені п'ятий, шостий, сьомий, восьмий, дев'ятий, десятий, одинадцятий, дванадцятий, тринадцятий та чотирнадцятий блоки постійної пам'яті, шостий, сьомий, восьмий, дев'ятий, десятий, одинадцятий, дванадцятий, тринадцятий, чотирнадцятий та п'ятнадцятий регістри. До блока керування додатково введені шостий, сьомий, восьмий, дев'ятий, десятий, одинадцятий, дванадцятий, тринадцятий, чотирнадцятий та п'ятнадцятий елементи І. Також додатково введені нові зв'язки у всьому пристрої.

Технічний результат, який може бути отриманий при використанні корисної моделі, полягає в одержанні технічного засобу для знаходження вихідного вектора при реалізації 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$ математичним способом.

На Фіг.1 приведена блок-схема запропонованого пристрою.

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

Запропонований пристрій для обчислення 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$ містить блок оперативної пам'яті 1, перший, другий, третій, четвертий, п'ятий, шостий, сьомий, восьмий, дев'ятий, десятий, одинадцятий, дванадцятий, тринадцятий та чотирнадцятий блоки постійної пам'яті 2-15, блок керування 16, перший мультиплексор 17, блок складання по модулю два 18, перший, другий, третій, четвертий, п'ятий, шостий, сьомий, восьмий, дев'ятий, десятий, одинадцятий, дванадцятий, тринадцятий та чотирнадцятий регістри 19-32, другий мультиплексор 33, п'ятнадцятий регістр 34, вхід запуску 35, вихід 36, причому вхід запуску 35 пристрою з'єднаний з входом блока керування. Адресні входи блока оперативної пам'яті 1 з'єднані з виходом 37 блока керування. Вхід дозволу читання блока оперативної пам'яті 1 з'єднаний з виходом 38 блока керування. Вихід блока оперативної пам'яті 1 з'єднаний з адресними входами блоків постійної пам'яті 2-15. Входи дозволу читання блоків постійної пам'яті 2-15 з'єднані з виходом 38 блока керування. Вихід блока постійної пам'яті 2 з'єднаний з першим входом мультиплексора 17. Вихід блока постійної пам'яті 3 з'єднаний з другим входом мультиплексора 17. Вихід блока постійної пам'яті 4 з'єднаний з третім входом мультиплексора 17. Вихід блока постійної пам'яті 5 з'єднаний з четвертим входом мультиплексора 17. Вихід блока постійної пам'яті 6 з'єднаний з п'ятим входом мультиплексора 17. Вихід блока постійної пам'яті 7 з'єднаний з шостим входом мультиплексора 17.

Вихід блока постійної пам'яті 8 з'єднаний з сьомим входом мультиплексора 17. Вихід блока постійної пам'яті 9 з'єднаний з восьмим входом мультиплексора 17. Вихід блока постійної пам'яті 10 з'єднаний з дев'ятим входом мультиплексора 17. Вихід блока постійної пам'яті 11 з'єднаний з десятиим входом мультиплексора 17. Вихід блока постійної пам'яті 12 з'єднаний з одинадцятим входом мультиплексора 17. Вихід блока постійної пам'яті 13 з'єднаний з дванадцятим входом мультиплексора 17. Вихід блока постійної пам'яті 14 з'єднаний з тринадцятим входом мультиплексора 17. Вихід блока постійної пам'яті 15 з'єднаний з чотирнадцятим входом мультиплексора 17. Адресні входи мультиплексора 17 з'єднані з виходом 39 блока керування. Вихід мультиплексора 17 з'єднаний з другим входом блока 18, що реалізує операцію складання по модулю два. Вихід блока 18, що реалізує операцію складання по модулю два, з'єднаний з входами даних регістрів 19-32. Входи дозволу запису регістрів 19-32 з'єднані з виходом 40 блока керування. Вихід регістра 19 з'єднаний з першим входом мультиплексора 33. Вихід регістра 20 з'єднаний з другим входом мультиплексора 33. Вихід регістра 21 з'єднаний з третім входом мультиплексора 33. Вихід регістра 22 з'єднаний з четвертим входом мультиплексора 33. Вихід регістра 23 з'єднаний з п'ятим входом мультиплексора 33. Вихід регістра 24 з'єднаний з шостим входом мультиплексора 33. Вихід регістра 25 з'єднаний з сьомим входом мультиплексора 33. Вихід регістра 26 з'єднаний з восьмим входом мультиплексора 33. Вихід регістра 27 з'єднаний з дев'ятим входом мультиплексора 33. Вихід регістра 28 з'єднаний з десятиим входом мультиплексора 33. Вихід регістра 29 з'єднаний з одинадцятим входом мультиплексора 33. Вихід регістра 30 з'єднаний з дванадцятим входом мультиплексора 33. Вихід регістра 31 з'єднаний з тринадцятим входом мультиплексора 33. Вихід регістра 32 з'єднаний з чотирнадцятим входом мультиплексора 33. Адресні входи мультиплексора 33 з'єднані з виходом 41 блока керування. Вихід мультиплексора 33 з'єднаний з входом даних регістра 34. Вхід дозволу запису регістра 34 з'єднаний з виходом 41 блока керування. Вихід регістра 34 є виходом 36 пристрою та з'єднаний з першим входом блока 18, що реалізує операцію складання по модулю два.

Блок керування 16 пристрою для обчислення 14-точкового усіченого перетворення Фур'є в полі GF(2⁸) містить: генератор тактових імпульсів 42, перший тригер 43, перший та другий лічильники 44 і 45, дешифратор 46, перший елемент І 47, формувач фронтів 48, перший та другий елементи АБО 49 і 50, третій та четвертий лічильники 51 і 52, другий та третій тригери 53 і 54, постійний запам'ятовуючий пристрій 55, другий, третій, четвертий, п'ятий, шостий, сьомий, восьмий, дев'ятий, десятий, одинадцятий, дванадцятий, тринадцятий, чотирнадцятий та п'ятнадцятий елементи І 56-69, причому вхід 35 блока керування з'єднаний з входом переводу тригера 43 в одиницю, вихід тригера 43 з'єднаний з входом генератора тактових імпульсів 42, вихід якого з'єднаний з рахунковим входом лічильника 45 та другими входами елементів І 56-69. Вхід скидання тригера 43 з'єднаний з виходом переповнення (переносу) лічильника 44. Перший вихід лічильника 45 (молодший розряд) з'єднаний з першим входом дешифратора 46 (молодший розряд) і першим входом елемента І 47. Другий вихід лічильника 45 з'єднаний з другим входом дешифратора 46. Третій вихід лічильника 45 з'єднаний з третім входом дешифратора 46 і другим входом елемента І 47. Четвертий вихід лічильника 45 з'єднаний з четвертим входом дешифратора 46 і третім входом елемента І 47. П'ятий вихід лічильника 45 (старший розряд) з'єднаний з п'ятим входом дешифратора 46 (старший розряд) і четвертим входом елемента І 47. Вихід елемента І 47 з'єднаний з входом формувача фронтів 48. Вихід формувача фронтів 48 з'єднаний з входом лічильника 44, входом обнуління лічильника 45, входами обнуління тригерів 53 і 54. Перший вихід дешифратора 46 з'єднаний з входом переводу тригера 53 в одиницю, другий вихід дешифратора 46 з'єднаний з входом переводу тригера 54 в одиницю, третій вихід дешифратора 46 з'єднаний з першим входом елемента АБО 49, четвертий вихід дешифратора 46 з'єднаний з першим входом елемента АБО 50 і першим входом елемента І 56, п'ятий вихід дешифратора 46 з'єднаний з другим входом елемента АБО 49, шостий вихід дешифратора 46 з'єднаний з другим входом елемента АБО 50 і першим входом елемента І 57, сьомий вихід дешифратора 46 з'єднаний з третім входом елемента АБО 49, восьмий вихід дешифратора 46 з'єднаний з третім входом елемента АБО 50 і першим входом елемента І 58, дев'ятий вихід дешифратора 46 з'єднаний з четвертим входом елемента АБО 49, десятий вихід дешифратора 46 з'єднаний з четвертим входом елемента АБО 50 і першим входом елемента І 59, одинадцятий вихід дешифратора 46 з'єднаний з п'ятим входом елемента АБО 49, дванадцятий вихід дешифратора 46 з'єднаний з п'ятим входом елемента АБО 50 і першим входом елемента І 60, тринадцятий вихід дешифратора 46 з'єднаний з шостим входом елемента АБО 49, чотирнадцятий вихід дешифратора 46 з'єднаний з шостим входом елемента АБО 50 і першим входом елемента І 61, п'ятнадцятий вихід дешифратора 46 з'єднаний з сьомим входом елемента АБО 49, шістнадцятий вихід дешифратора 46 з'єднаний з сьомим входом елемента АБО 50 і першим входом елемента І 62, сімнадцятий вихід дешифратора 46 з'єднаний з восьмим входом елемента АБО 49, вісімнадцятий вихід дешифратора 46 з'єднаний з восьмим входом елемента АБО 50 і першим входом елемента І 63, дев'ятнадцятий вихід дешифратора 46 з'єднаний з дев'ятим входом елемента АБО 49, двадцятий вихід дешифратора 46 з'єднаний з дев'ятим входом елемента АБО 50 і першим входом елемента І 64, двадцять перший вихід дешифратора 46 з'єднаний з десятиим входом елемента АБО 49, двадцять другий вихід дешифратора 46 з'єднаний з десятиим входом елемента АБО 50 і першим входом елемента І 65, двадцять третій вихід дешифратора 46 з'єднаний з одинадцятим входом елемента АБО 49, двадцять четвертий вихід дешифратора 46 з'єднаний з одинадцятим входом елемента АБО 50 і першим входом елемента І 66, двадцять п'ятий вихід дешифратора 46 з'єднаний з дванадцятим входом елемента АБО 49, двадцять шостий вихід дешифратора 46 з'єднаний з дванадцятим входом елемента АБО 50 і першим входом елемента І 67, двадцять сьомий вихід дешифратора 46 з'єднаний з тринадцятим входом елемента АБО 49, двадцять восьмий вихід дешифратора 46 з'єднаний з тринадцятим входом елемента АБО 50 і першим входом елемента І 68, двадцять дев'ятий вихід дешифратора 46 з'єднаний з чотирнадцятим входом елемента АБО 49, тридцятий вихід дешифратора 46 з'єднаний з чотирнадцятим входом елемента АБО 50 і першим входом елемента І 69. Вихід елемента АБО 49 з'єднаний з тактовим входом лічильника 51. Вихід елемента АБО 50 з'єднаний з тактовим входом лічильника 52. Виходи лічильника 52 з'єднані з входами постійного запам'ятовуючого пристрою 55. Виходи лічильника 44 по виходу 37 блока керування 16 з'єднані з адресними входами блока оперативної пам'яті 1. Вихід тригера 53 по виходу 38 блока керування 16 з'єднаний з входом дозволу читання блока оперативної

пам'яті 1. Вихід тригера 54 по виходу 38 блока керування 16 з'єднаний з входами дозволу читання блоків постійної пам'яті 2-15. Виходи постійного запам'ятовуючого пристрою 55 по виходу 39 блока керування 16 з'єднані з адресними входами мультиплексора 17. Вихід елемента І 56 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 19. Вихід елемента І 57 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 20. Вихід елемента І 58 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 21. Вихід елемента І 59 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 22. Вихід елемента І 60 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 23. Вихід елемента І 61 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 24. Вихід елемента І 62 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 25. Вихід елемента І 63 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 26. Вихід елемента І 64 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 27. Вихід елемента І 65 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 28. Вихід елемента І 66 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 29. Вихід елемента І 67 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 30. Вихід елемента І 68 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 31. Вихід елемента І 69 по виходу 40 блока керування 16 з'єднаний з входом дозволу запису регістра 32. Вихід елемента АБО 49 по виходу 41 блока керування 16 з'єднаний з входом дозволу запису регістра 34. Виходи лічильника 51 по виходу 41 блока керування 16 з'єднані з адресними входами мультиплексора 33.

Робота запропонованого пристрою здійснюється за 14 циклів по 30 тактів в кожному та полягає в наступному. Перед початком роботи в блок оперативної пам'яті 1 записаний вхідний вектор $v = \{v_1, v_2, \dots, v_{14}\}$ в двійковому коді, причому $v_i \in GF(2^8)$.

В блоки постійної пам'яті 2-15 за адресою $v_i = 0 \div 255$ записані результати множення в полі $GF(2^8)$ у виді

$$\{P(v_i \cdot w^{ij})\},$$

де $P(X)$ - перехід від десяткового представлення елемента поля $GF(2^8)$ до двійкового представлення;

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

i - номер точки вхідного вектору;

j - номер точки вихідного вектору.

Регістри 19-32, регістр 34, тригер 43, лічильники 44, 45, 51, 52, тригери 53 і 54 у нульовому стані.

На виході дешифратора 46 під час роботи пристрою формується унітарний код такту, причому рівень "1" буде тільки на одному з його виходів.

Постійний запам'ятовуючий пристрій 55 містить для кожного з тактів 4, 6, ..., 30 циклів 1-14 адреси, що використовують для адресації мультиплексора 17 з метою здійснення математичного способу знаходження вихідного вектора при реалізації 14-точкового усіченого перетворення Фур'є в полі $GF(2^8)$.

По сигналу "Запуск обробки", що надходить по входу 35 пристрою, тригер 43 встановлюється в одиничний стан, сигнал "1" з виходу тригера 43 надходить на вхід генератора тактових імпульсів 42, що починає формувати послідовність тактових імпульсів, які надходять на рахунковий вхід лічильника 45 та другі входи елементів І 56 - І 69.

Цикл 1.

На першому такті формується рівень "1" на першому виході дешифратора 46, що встановлює тригер 53 в одиницю. Рівень "1" з виходу тригера 53 через вихід 38 блока керування 16 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 46, що встановлює тригер 54 в одиницю. Рівень "1" з виходу тригера 54 через вихід 38 блока керування 16 поступає на входи дозволу читання блоків постійної пам'яті 2-15. При цьому на виходах блоків постійної пам'яті 2-15 формується двійкове представлення результату множення $v_i \cdot w^{ij}$ у полі $GF(2^8)$. Двійкове представлення результату множення з виходу відповідного блока постійної пам'яті (2-15) через мультиплексор 17 поступає на другий вхід блока 18. З виходу блока 18 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 34, поступає на входи даних регістрів 19-32.

На третьому такті формується рівень "1" на третьому виході дешифратора 46, що з виходу елемента АБО 49 через вихід 41 блока керування 16 по передньому фронту імпульсу в регістр 34 через мультиплексор 33 записує значення, що міститься у регістрі 19. По задньому фронту імпульсу з виходу елемента АБО 49 лічильник 51 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 51 через вихід 41 блока керування 16 поступає на адресні входи мультиплексора 33 та комує на вхід даних регістра 34 вихід регістра 20.

На четвертому такті формується рівень "1" на четвертому виході дешифратора 46, що з виходу елемента І 56 через вихід 40 блока керування 16 записує до регістра 19 результат складання по модулю два результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 34. Рівень "1" з четвертого виходу дешифратора 46 поступає на елемент АБО 50. По передньому фронту імпульсу з виходу елемента АБО 50 лічильник 52 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 55 через вихід 39 блока керування 16 на адресних входах мультиплексора 17 встановлюється новий адрес і двійкове представлення результату множення v_1 у полі $GF(2^8)$ з виходу відповідного блока постійної пам'яті (2-15) через мультиплексор 17 поступає на другий вхід блока 18. З виходу блока 18 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 34, поступає на входи даних регістрів 19-32.

На п'ятому такті формується рівень "1" на п'ятому виході дешифратора 46, що з виходу елемента АБО 49 через вихід 41 блока керування 16 по передньому фронту імпульсу в регістр 34 через мультиплексор 33 записує значення, що міститься у регістрі 20. По задньому фронту імпульсу з виходу елемента АБО 49 лічильник 51 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 51 через вихід 41 блока керування 16 поступає на адресні входи мультиплексора 33 та комує на вхід даних регістра 34 вихід регістра 21.

На шостому такті формується рівень "1" на шостому виході дешифратора 46, що з виходу елемента І 57

запам'ятовуючого пристрою 55 через вихід 39 блока керування 16 на адресних входах мультиплексора 17 встановлюється новий адрес і двійкове представлення результату множення v_1 у полі $GF(2^8)$ з виходу відповідного блока постійної пам'яті (2-15) через мультиплексор 17 поступає на другий вхід блока 18. З виходу блока 18 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 34, поступає на входи даних регістрів 19-32.

На двадцять п'ятому такті формується рівень "1" на двадцять п'ятому виході дешифратора 46, що з виходу елемента АБО 49 через вихід 41 блока керування 16 по передньому фронту імпульсу в регістр 34 через мультиплексор 33 записує значення, що міститься у регістрі 30. По задньому фронту імпульсу з виходу елемента АБО 49 лічильник 51 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 51 через вихід 41 блока керування 16 поступає на адресні входи мультиплексора 33 та комутує на вхід даних регістра 34 вихід регістра 31.

На двадцять шостому такті формується рівень "1" на двадцять шостому виході дешифратора 46, що з виходу елемента І 67 через вихід 40 блока керування 16 записує до регістра 30 результат складання по модулю два результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 34. Рівень "1" з двадцять шостого виходу дешифратора 46 поступає на елемент АБО 50. По передньому фронту імпульсу з виходу елемента АБО 50 лічильник 52 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 55 через вихід 39 блока керування 16 на адресних входах мультиплексора 17 встановлюється новий адрес і двійкове представлення результату множення v_1 у полі $GF(2^8)$ з виходу відповідного блока постійної пам'яті (2-15) через мультиплексор 17 поступає на другий вхід блока 18. З виходу блока 18 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 34, поступає на входи даних регістрів 19-32.

На двадцять сьомому такті формується рівень "1" на двадцять сьомому виході дешифратора 46, що з виходу елемента АБО 49 через вихід 41 блока керування 16 по передньому фронту імпульсу в регістр 34 через мультиплексор 33 записує значення, що міститься у регістрі 31. По задньому фронту імпульсу з виходу елемента АБО 49 лічильник 51 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 51 через вихід 41 блока керування 16 поступає на адресні входи мультиплексора 33 та комутує на вхід даних регістра 34 вихід регістра 32.

На двадцять восьмому такті формується рівень "1" на двадцять восьмому виході дешифратора 46, що з виходу елемента 168 через вихід 40 блока керування 16 записує до регістра 31 результат складання по модулю два результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 34. Рівень "1" з двадцять восьмого виходу дешифратора 46 поступає на елемент АБО 50. По передньому фронту імпульсу з виходу елемента АБО 50 лічильник 52 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 55 через вихід 39 блока керування 16 на адресних входах мультиплексора 17 встановлюється новий адрес і двійкове представлення результату множення v_1 у полі $GF(2^8)$ з виходу відповідного блока постійної пам'яті (2-15) через мультиплексор 17 поступає на другий вхід блока 18. З виходу блока 18 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 34, поступає на входи даних регістрів 19-32.

На двадцять дев'ятому такті формується рівень "1" на двадцять дев'ятому виході дешифратора 46, що з виходу елемента АБО 49 через вихід 41 блока керування 16 по передньому фронту імпульсу в регістр 34 через мультиплексор 33 записує значення, що міститься у регістрі 32. По задньому фронту імпульсу з виходу елемента АБО 49 лічильник 51 встановлюється в 0. Двійковий код з виходу лічильника 51 через вихід 41 блока керування 16 поступає на адресні входи мультиплексора 33 та комутує на вхід даних регістра 34 вихід регістра 19.

На тридцятому такті формується рівень "1" на тридцятому виході дешифратора 46, що з виходу елемента І 69 через вихід 40 блока керування 16 записує до регістра 32 результат складання по модулю два результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 34. Рівень "1" з тридцятого виходу дешифратора 46 поступає на елемент АБО 50. По передньому фронту імпульсу з виходу елемента АБО 50 лічильник 52 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 55 через вихід 39 блока керування 16 на адресних входах мультиплексора 17 встановлюється новий адрес і двійкове представлення результату множення v_1 у полі $GF(2^8)$ з виходу відповідного блока постійної пам'яті (2-15) через мультиплексор 17 поступає на другий вхід блока 18. З виходу блока 18 результат складання по модулю два результату множення зі значенням, що міститься на виході регістра 34, поступає на входи даних регістрів 19-32. По задньому фронту імпульсу з виходу елемента І 47 через формувач фронтів 48 здійснюється збільшення на одиницю лічильника 44, обнуління лічильника 45 та встановлення в "0" тригерів 53 і 54. Двійковий код з виходу лічильника 44 через вихід 37 блока керування 16 встановлює на адресних входах блока оперативної пам'яті 1 адресу для зчитування двійкового представлення числа v_2 .

Цикли 2, 3, ..., 14 здійснюються аналогічно циклу 1 за винятком того, що всі операції здійснюються з використанням двійкового представлення чисел $v_2, v_3, \dots, v_{14}$ відповідно.

Після завершення останнього такту чотирнадцятого циклу на виході переповнення лічильника 44 формується рівень "1", що скидає тригер 43 у нульовий стан, а пристрій повертається у початковий стан, при цьому з виходу 36 пристрою через мультиплексор 33 і регістр 34 зчитують остаточний результат, що міститься на виходах регістрів 19-32.

Джерела інформації

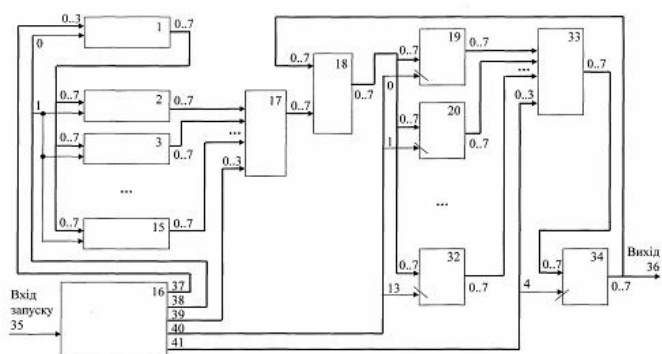
1. А.с. 1569847 СССР, МКИ G06F15/332. Устройство для быстрого действительного преобразования Хартли-Фур'е / С.Н. Демиденко, Э.Б. Куновский, О.В. Малашонок, Е.М. Левин. - №4473106; Заяв.10.08.88, Оpubл.7.06.90, Бюл. №21.

2. Деклараційний патент №4264 У України, 7МПК G06F7/04. Пристрій для обчислення усіченого перетворення Фур'є в остаточних класах / Дуденко С.В., Рубан І.В., Третяк В.Ф., Сумцов Д.В. - №2004032321; Заяв.30.03.2004, Оpubл.17.01.2005, Бюл. №1. - 4с. ил.

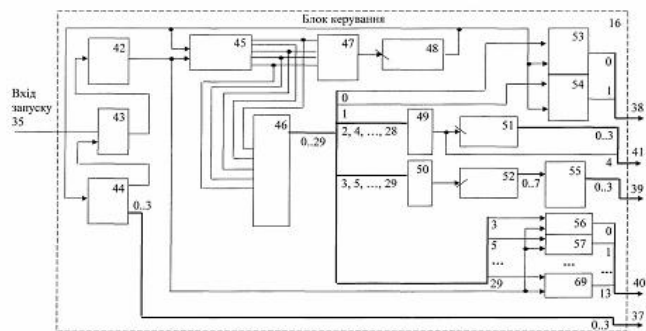
3. Деклараційний патент на корисну модель №14431U України, МПК(2006) G06F5/00 G06F17/14. Пристрій для

обчислення усіченого пере творення Фур'є в залишкових класах / Дуденко СВ., Рубан І.В., АлексєєвС.В., Колмиков М.М., Калачова В.В. - №и200510997; Заяв.21.11.2005, Опубл. 15.05.2006, Бюл. №5. - 6с іл.

4. Рубан І.В., Дуденко СВ. Оптимизация теоретико-числовых преобра зований // Інформаційно-керуючи системи на залізничному транспорті. - 2002. - №6. – С.47-49.



Фиг. 1



Фиг. 2