Vol. 3, No. 1, 2021

DOI: https://doi/org/10.23939/csn2021. 01.007

УДК 681.32

УДОСКОНАЛЕННЯ СТРУКТУР БАГАТОРОЗРЯДНИХ ПЕРЕМНОЖУВАЛЬНИХ ПРИСТРОЇВ У РІЗНИХ ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСАХ

[1]Н. Я. Возна, [1]А. Я. Давлетова, [1]Я. М. Николайчук, [2]В. М. Грига

[1]Західноукраїнський національний університет, кафедра спеціалізованих комп'ютерних систем

[2]Прикарпатський національний університет імені В.Стефаника, кафедра обчислювальної техніки та електроніки

E-mail: nvozna@ukr.net

У статті запропоновано методи удосконалення структур багаторозрядних перемножувачів, які характеризуються підвищеною швидкодією, зменшеною структурною складністю пристрою та зменшеною структурною складністю входо-виходів у залежності від розрядності перемножувачів (512-2048 біт) відповідно у (1024-4096) разів, у порівнянні з відомими перемножувачами на основі класичних однорозрядних повних суматорів. Запропоновано оптимізацію структур багаторозрядних перемножувачів. Наведено порівняльні оцінки структурної, функціональної та відносної функціонально-структурної складностей їх схемотехнічних реалізацій. Застосування оптимізованих схемотехнічних рішень перемножувачів дозволяє значно покращити системні характеристики складних обчислювальних пристроїв з великою кількістю таких компонентів у кристалах мікроелектронних технологій.

Ключові слова – багаторозрядні перемножувальні пристрої, структурна складність, удосконалення структур.

Стан проблеми

Відповідно до теоретичних основ та концепції вирішення задач структуризації даних в інформаційних кіберфізичних системах [1], актуальною є проблема, яка охоплює: розроблення методів структурної оптимізації системних характеристик компонентів багаторозрядних спецпроцесорів, які забезпечують можливість підвищення швидкодії, зменшення апаратної складності та спрощення задач цифрового опрацювання сигналів.

Арифметична операція множення застосовується у великій кількості алгоритмів опрацювання сигналів та обчислень. Така операція, а особливо компоненти, які її реалізують, є ваговим атрибутом, який суттєво впливає на апаратну. структурну складність та, відповідно, на продуктивність багаторозрядних обчислювальних пристроїв.

Постановка задачі

Такі обчислювальні пристрої як перемножувачі, квадратори широко застосовуються у якості базових структурних компонентів обчислювальних засобів, які реалізують статистичні, кореляційні, спектральні, ентропійні, кластерні моделі у розподілених системах керування, регулювання та моніторингу.Кількість відповідних компонентів може складати 3-6 порядків в системах реального часу. Тому до них висуваються жорсткі вимоги згідно критеріїв мінімальної апаратної, часової, структурної та максимальної поліфункціональної складності.

Відповідно удосконалення системних характеристик перемножувачів є актуальною науково-прикладною задачею їх мікроелектронного синтезу на кристалах.

Результати досліджень

1. Перемножувач унітарних кодів у базисі Хаара-Крестенсона.

Перемножувачі унітарних кодів широко застосовуються для паралельного цифрового опрацювання кодів RGB-пікселів відеокамер [2]. У стандартних відеокамерах у залежності від їх призначення загальна кількість реєстрованих RGB-пікселів може складати $2^{20} - 2^{30}$, наприклад кольорове зображення – 512×512 ($8+8+8=24$) біт/піксель; CCIR TV – $720 \times 576 \times 30$ ($8+8+8=24$) біт/піксель; HDTV – $1280 \times 720 \times 60$ ($8+8+8=24$) біт/піксель. Тому зменшення структурної складності та підвищення швидкодії таких компонентів цифрових відеозасобів є актуальною проблемою.

Запропоноване удосконалення структури унітарного перемножувача [3], який здійснює операції перемноження у базисі Хаара-Крестенсона та дозволяє на один порядок підвищити його швидкодію у порівнянні з відомим пристроєм [4], а також забезпечити більш високу регулярність структури за рахунок застосування матрично-модульних компонентів на елементах "І-НЕ".

На рис.1 [3] показана структурна схема пристрою, де 1, 3 –вхідні шини унітарних кодів; 2, 4 – модульні лічильники Джонсона на D-тригерах; 5 –матриці модульного перемноження; 6 – шифратор, який перетворює коди Хаара-Крестенсона у двійкові коди базису Радемахера.

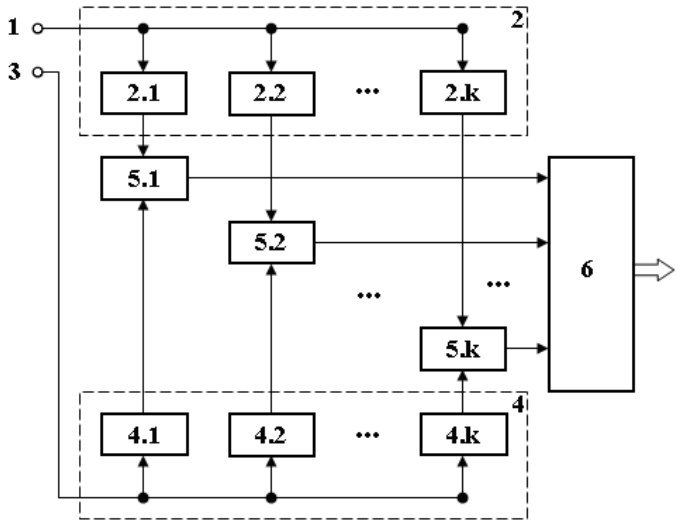


Рис.1. Структурна схема числоімпульсного множильного пристрою у базисі Хаара-Крестенсона

Структурна складність множильного пристрою визначається сумарною оцінкою складностей лічильника на D-тригерах ($k_{сЛ}$), матриці модульного перемноження ($k_{сМП}$) та шифратора ($k_{сШ}$) згідно виразу: $k_c = k \cdot (2k \cdot k_{сЛ} + k_{сМП}) + k_{сШ}$.

При $k = 8$ та наборі модулів: $P_1 = 5$, $P_2 = 7$, $P_3 = 8$ структурна складність компонентів становитиме:

$$k_{сЛ} = (2 \cdot \sum_{i=1}^{k} (P_1 + P_2 + ...P_k)) \cdot k_{сТ} = 2 \cdot (5+7+8) \cdot 30 = 1200;$$

$$k_{сМП} = k \cdot (P_1^2 + P_2^2 + ... + P_k^2) \cdot k_{сІ-НЕ} + \sum_{i=1}^{k} (P_1 + P_2 + ... + P_k) \cdot k_{сНЕ} =$$

$$= 8 \cdot (5+7+8) \cdot 14,4 + (5+7+8) \cdot 14,8 = 2304 + 296 = 2600$$

$$k_{сш} = 2^{k}(4 \div 5) + 2^{k}(\sum_{i=1}^{n} P_i) = 2^{8} \cdot (4 \div 5) + 2^{8} \cdot (5 + 7 + 8) = 256 \cdot (4 \div 5) + 256 \cdot 20 =$$

$$= 1024 \div 1280 + 5120 = 6144 \div 6400.$$

Таким чином сумарна оцінка структурної складності множильного пристрою становить:

$k_c = 8 \cdot (2 \cdot 8 \cdot 1200 + 2600) + 6144 = 180544$ одиниць.

Розрахунок системи взаємнопростих модулів $P_1, P_2, ..., P_i, ..., P_k$ для числоімпульсного множильного пристрою при $k = 8$ виконується виходячи з умови, що добуток модулів $P_1, P_2, ..., P_i, ..., P_k$ повинен перевищувати числове значення 2^{16}. Цій умові відповідає наступний набір модулів системи залишкових класів базису Крестенсона $P_1 = 7$, $P_2 = 8$, $P_3 = 9$, $P_4 = 11$, $P_3 = 13$; $7 \cdot 8 \cdot 9 \cdot 11 \cdot 13 = 72072 > 2^{16} = 65536$. Таким чином на виходах матричних модульних перемножувачів, після завершення процесу множення, формується код Хаара-Крестенсона $d_1, d_2, ..., d_5$, який дешифрується у 16-тирозрядний двійковий код базису Радемахера.

Приклад: Нехай перемножуються числа $X = 100$, $Y = 200$; $X \cdot Y = 20000$.

Числа *X* та *Y* представляються у базисі Хаара-Крестенсона наступним кодом:

X= res 100(mod 7)=a1=2 = 0010000
res 100(mod 8)=a2=4 = 00001000
res 100(mod 9)=a3=1 = 010000000
res 100(mod 11)=a4=1=01000000000
res 100(mod 13)=a5=9=0000000001000

Y= res 200(mod 7)=b1=4 = 0000100
res 200(mod 8)=b2=0 = 00000000
res 200(mod 9)=b3=2 = 001000000
res 200(mod 11)=b4=2=00100000000
res 200(mod 13)=b5=5=0000010000000

Сформовані таким чином коди поступають на входи *i*-тих матричних модульних перемножувачів, на виходах яких формується код Хаара-Крестенсона результатів перемноження $d_1, d_2, ..., d_k$ згідно виразу: $(a_i \cdot b_i) \bmod P_i = d_i$,

P_i	7	8	9	11	13
a_i =	(2	4	1	1	9)
b_i =	(4	0	2	2	5)
d_i =	(1	0	2	2	6);

що відповідає дешифрованому значенню 20000 у двійковій системі числення базису Радемахера 100111000100000.

d=20000
res 20000(mod 7)=a_1 = 1
res 20000(mod 8)=a_2 = 0
res 20000(mod 9)=a_3 = 2
res 20000(mod 11)=a_4=2
res 20000(mod 13)=a_5=6.

З метою спрощення структури шифратора (6), його слід реалізувати по двокаскадній схемі: в першому каскаді коди Хаара-Крестенсона по кожному модулю перетворюються в двійкові коди Радемахера, які в другому каскаді перетворюються в позиційний код двійкової системи числення. Тобто 48-мибітний код Хаара-Крестенсона дешифрується у 18-тибітний код Радемахера-Крестенсона та 16-тибітний код Радемахера. При цьому в шифраторі (6) затримка сигналів складає 4υ і загальна швидкодія пристрою складає $6 + 2 = 8\upsilon$.

Перемножувач унітарних кодів у базисі Хаара-Крестенсона характеризується підвищеною на 1 порядок швидкодією по відношенню до відомого пристрою, а також більш високою регулярністю

структури за рахунок реалізації модульних лічильників на регістрах зсуву, та матричних модульних перемножувачів на елементах "І-НЕ".

2. Структура та системні характеристики швидкодіючого різницево-модульного квадратора у кодах Хаара-Крестенсона

Реалізація процесора визначення Хеммінгової віддалі згідно квадратичної Евклідової відстані потребує застосування операції піднесення до квадрату кодів модульних різниць аналогових сигналів, що потребує застосування матричних перемножувачів та приводить до суттєвого зниження швидкодії, зростання апаратної та структурної складності такого класу процесорів у базисі Радемахера. Тому запропонована структурна схема різницево-модульного квадратора [5], який є компонентом пристрою визначення Хеммінгової віддалі і реалізується у кодах базису Хаара-Крестенсона.

Такий різницево-модульний квадратор застосовується в якості швидкодіючого компонента при вирішенні задач статистичного аналізу та реалізації високопродуктивних компонентів спецпроцесорів визначення Хеммінгової віддалі згідно квадратичної оцінки Евклідової відстані.

Структура високопродуктивного спецпроцесора містить 2 АЦП паралельного типу з вихідними кодами у базисі Хаара-Крестенсона, реалізована шляхом застосування модульної арифметики СЗК та кодових матриць Хаара-Крестенсона (рис.2) [5].

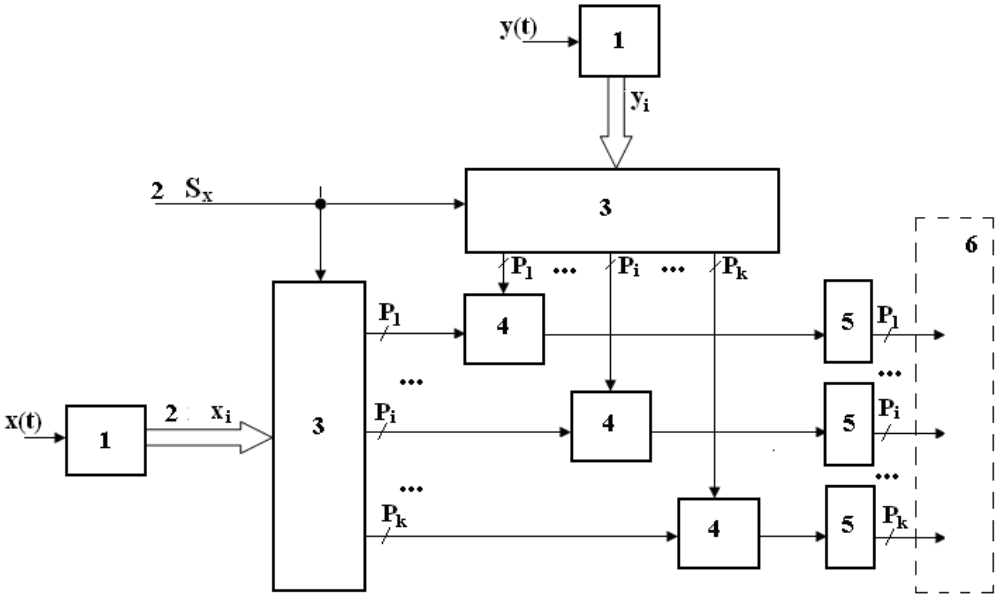


Рис.2. Структурна схема різницево-модульного квадратора

Різницево-модульний квадратор (рис.2) містить: АЦП паралельного типу (1) з відповідними вихідними кодами Хаара-Крестенсона x_i та y_i ($x_i = (a_1, a_2, ...a_i, ..., a_k)$, $y_i = (b_1, b_2, ...b_i, ..., b_k)$; $a_i = resx_i (\mathrm{mod}\, P_i)$, $b_i = resy_i (\mathrm{mod}\, P_i)$; $i \in \overline{1,k}$, k – кількість модулів кодів Хаара-Крестенсона), шину синхронізації S_x (2), яка формує сигнали запису кодів x_i та y_i у регістрі пам'яті на D-тригерах (3), матриці визначення модульних різниць по кожному P_i модулю (4), модульні квадратори у базисі Хаара-Крестенсона (5), вихідну шину (6).

На рис.3 показаний приклад реалізації та структура з'єднання вентилів входів та виходів різницево-модульної матриці на логічних елементах "І-НЕ" ($P = 7$).

На рис.4 показана структурна реалізація формування коду квадрату модульної різниці ($(a_i - b_i)^2 \bmod P_i$) у базисі Хаара-Крестенсона на логічних елементах "І-НЕ" ($P = 7$).

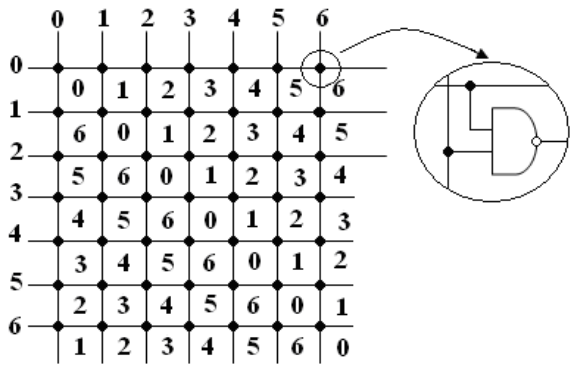


Рис.3. Різницево-модульна матриця на елементах "I-НЕ"

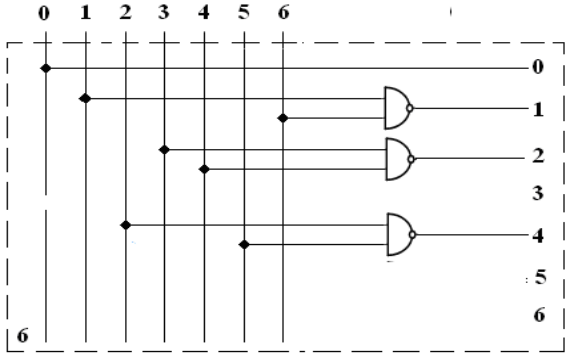


Рис.4. Реалізації формування коду квадрату модульної різниці ($(a_i - b_i)^2 \bmod P_i$) у базисі Хаара-Крестенсона.

Згідно з властивостями системи числення залишкових класів для однозначного представлення квадрату різниці двох чисел $(x_i - y_i)^2$ повинна виконуватися умова: добуток P_0 взаємно-простих модулів P_i повинен бути рівний або більший $N = [(x_i - y_i)\max]$, що відповідає умові: сума двійкових розрядностей модулів P_i повинна бути на 1-2 розряди більша відносно кількості розрядів двійкового представлення максимального квадрату різниці між числами x_i та y_i, тобто: $n \geq \hat{E}[\log_2 N^2]$, де $\hat{E}$ – цілочисельна функція з округленням до більшого цілого. Наприклад, при кількості модулів P_i, $k = 4$ і максимальних значеннях квадратів N. Розрахунки для різних N показано в таблиці 1.

Таблиця 1

Приклад максимальних значень квадратів N

		P_1	P_2	P_3	P_4	n	N^2	P_0
N	15	2	3	5	11	9	225	330
n	4	1	2	3	4			
N	99	8	9	11	13	15	9801	10296
n	7	3	4	4	4			
N	255	13	16	17	19	18	65025	67194
n	8	4	4	5	5			
N	1023	29	32	33	37	22	1046529	1133088
n	10	5	5	6	6			
N	2047	43	45	47	49	24	4190209	4456305
n	12	6	6	6	6			

Особливістю роботи пристрою є незалежність формування прямого коду квадрату на виходах модулів квадраторів (5), незалежно від того прямі чи інвертовані коди по модулю формуються на виходах різницево-модульних матриць (4).

Наприклад: необхідно визначити квадрат різниці між двома числами, які можуть бути представлені у діапазоні: $0 \leq x_i \leq 127$, $0 \leq y_i \leq 127$, максимальне значення квадрату їх різниць рівне $127^2 = 16129$.

Представимо за дані числа $x_i = 101$, $y_i = 65$, у базисах Радемахера-Крестенсона та Хаара-Крестенсона у системі числення залишкових класів з набором модулів: $P_1 = 4$, $P_2 = 5$, $P_3 = 7$, $P_4 = 9$,

$P_4 = 13$. Добуток модулів рівний $4 \cdot 5 \cdot 7 \cdot 9 \cdot 13 = 16380 > 16129$. У кодах Радемахера-Крестенсона задані числа становитимуть: $x_i = 101_{10} = (1\ \ 1\ \ 3\ \ 2\ \ 10)_{(4,5,7,9,13)}$, $y_i = 65_{10} = (1\ \ 0\ \ 2\ \ 2\ \ 0)_{(4,5,7,9,13)}$. Виконаємо віднімання заданих чисел в системі залишкових класів і піднесення до квадрату отриманих різниць:

P_i	4	5	7	9	13
x_i	1	1	3	2	10
y_i	1	0	2	2	0
$x_i - y_i$	0	1	1	0	10
	0	1	1	0	10
$\lvert x_i - y_i \rvert^2$	0	1	1	0	9

P_i	4	5	7	9	13
y_i	1	0	2	2	0
x_i	1	1	3	2	10
$y_i - x_i$	0	4	6	0	3
	0	4	6	0	3
$\lvert y_i - x_i \rvert^2$	0	1	1	0	9

Тобто отримані результати кодів квадратів, які рівні між собою. В кодах Хаара-Крестенсона по кожному модулю P_i дані операції виконуються на різницево-модульних матрицях (4) та логічних модулях квадраторів (5). У результаті отримується наступний код Хаара-Крестенсона: 0 1 1 0 9, що рівне числу 1296.

Така властивість квадратів кодів Хаара-Крестенсона дозволяє спростити реалізацію двох послідовно з'єднаних компонентів спецпроцесора Хаара-Крестенсона шляхом безпосереднього використання вихідних прямих та доповнюючих кодів різницево-модульних матриць (4) та заміни логічних елементів "АБО" відповідними логічними елементами "І-НЕ" на основі модульних квадраторів (5).

Загальна затримка сигналів у розробленому спецпроцесорі визначення квадратів модульних різниць між двома вхідними аналоговими сигналами, незалежно від розрядності вхідних чисел, складає 8 мікротактів.

Структурна складність розробленого спецпроцесора розраховується згідно виразу:

$$k_{c2} = k_{cAЦП} + 2 \cdot k_{cP} + k \cdot k_{cM} + k \cdot k_{cK},$$

де $k_{cAЦП} = 2^{\mathrm{k}} \cdot (k_{cK} + k_{cI-HE1}) + \sum_{i=1}^{k} (P_1 + P_2 + P_3 + P_4) \cdot k_{cI-HE1}$, $k_{cP} = \sum_{i=1}^{k} P_i \cdot k_{cT}$; $k_{cM} = \sum_{i=1}^{k} (P_i)^2 \cdot k_{cI-HE}$;

$k_{cK} = \sum_{i=1}^{k} \frac{P_i}{2} \cdot k_{cI-HE}$, де k_{cP} – структурна складність регістра на D-тригерах; k_{cM} – структурна складність різницево-модульної матриці; k_{cK} – структурна складність модулів квадраторів.

Таким чином, при $k = 8$, де

$$k_{cAЦП} = 2^{\mathrm{k}} \cdot (k_{cK} + k_{cI-HE1}) + \sum_{i=1}^{k} (P_1 + P_2 + P_3 + P_4) \cdot k_{cI-HE1} = 40838;$$

$$k_{cP} = \sum_{i=1}^{k} P_i \cdot k_{cT} = (5 + 7 + 8) \cdot 30 = 600;$$

$$k_{cM} = \sum_{i=1}^{k} (P_i)^2 \cdot k_{cI-HE} = (5 + 7 + 8)^2 \cdot 14,4 = 5760;$$

$$k_{cK} = \sum_{i=1}^{k} \frac{P_i}{2} \cdot k_{cI-HE} = \frac{5 + 7 + 8}{2} \cdot 14,4 = 144.$$

Отже,

$$k_{c2} = k_{cAЦП} + 2 \cdot k_{cP} + k \cdot k_{cM} + k \cdot k_{cK} = 40838 + 2 \cdot 600 + 8 \cdot 5760 + 8 \cdot 144 = 89270.$$

В частковому випадку, коли одне з чисел x_i або y_i є нульовим, пристрій реалізує функцію піднесення до квадрату одного числа у базисі Хаара-Крестенсона.

При діапазоні кодування вхідних чисел $N = 255$, що відповідає кількості рівнів квантування окремих кольорів RGB-пікселів, запропонований пристрій дозволяє реалізувати визначення Хеммінгової віддалі між пікселями кожного з кольорів зображень. При накопиченні кодів отриманих окремих різницевих квадратів, згідно матриці пікселів відео зображення, реалізується можливість розпізнавання двох зображень на основі інтегральної оцінки Хеммінгової віддалі у квадратичному Евклідовому просторі.

3. Матричний перемножувач

Відомий матричний перемножувач Брауна з горизонтальним та вертикальним розповсюдженням переносу [6, 7]. Біти часткових добутків виду ($a_i b_i$) формуються за допомогою елементів ”І”. Для сумування часткових добутків застосовуються два види однорозрядних суматорів із збереженням переносу: напівсуматори (НС) і повні суматори (СМ).

При застосуванні класичних схем неповного та повного однорозрядних двійкових суматорів час затримки вихідного переносу неповного суматора складає 1 мікротакт, а повного 2-5 мікротактів, а час формування суми складає 3 мікротакти для неповного суматора і 6 мікротактів для повного суматора [8].

Оцінка часової складності матричного перемножувача розраховується з врахуванням горизонтальних затримок сигналів наскрізних переносів та вертикальних затримок сигналів при формуванні бітів суми. Тобто системні характеристики часової складності відомих однорозрядних двійкових суматорів з горизонтальними (+) і вертикальними (s) інформаційними зв’язками відповідно складають:

$$\tau_{МП} = 2\tau_{НС} + (3n-6)\cdot\tau_{ПС} = 2\cdot 3 + (3\cdot 4 - 6)\cdot 6 = 42\,\upsilon\,.$$

Оцінка апаратної складності матричного перемножувача розраховується з врахуванням кількості логічних елементів, які містять однорозрядні двійкові суматори, становить:

$$A_{МП} = n\cdot A_{НС} + (n^2 - 2n)\cdot A_{ПС} = 4\cdot 5 + (4^2 - 2\cdot 4)\cdot 11 = 108\,V\,.$$

Оцінка структурної складності матричного перемножувача становить $S_{МП} = 1026$ одиниць.

Недоліком матричного перемножувача Брауна є обмежені функціональні можливості та низька швидкодія, яка обумовлена тим, що базовий компонент матриці однорозрядних суматорів не містить парафазних входів та виходів, що потребує не менше $2 \div 3$ мікротакти часової затримки сигналів переносів і не дозволяє, у принципі, реалізувати відповідні вертикальні та горизонтальні переноси між виходами та входами однорозрядних суматорів з часовою затримкою 1 мікротакт.

Запропонована у [9] структура матричного перемножувача багаторозрядних двійкових чисел на основі парафазних однорозрядних суматорів, представлена на рис.5.

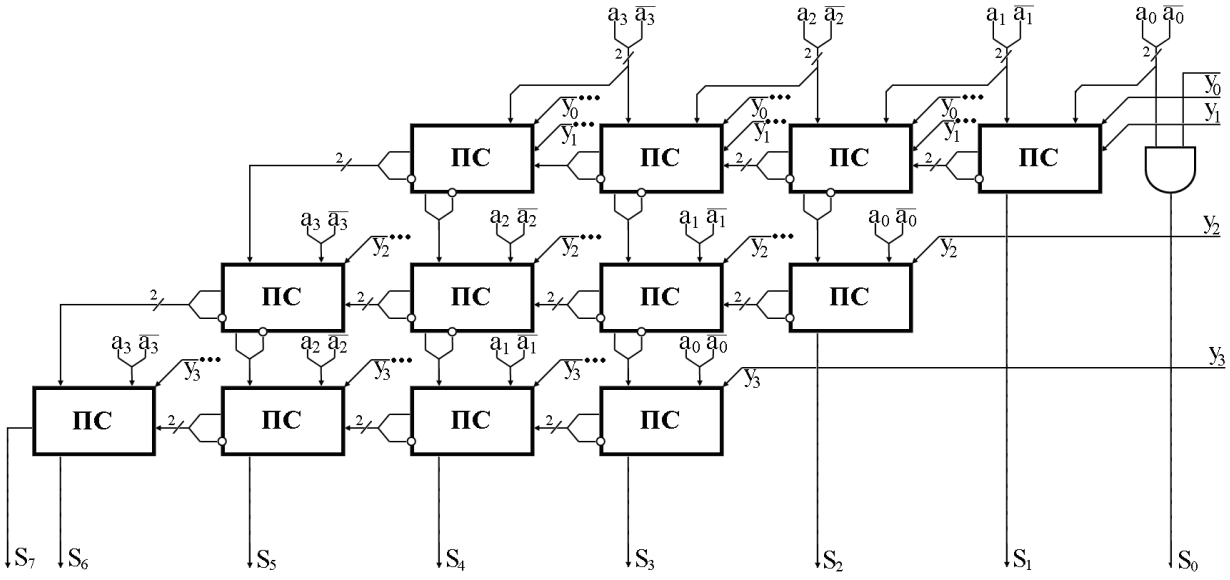


Рис.5. Структура матричного перемножувача
на основі комутованих парафазних однорозрядних суматорів

Дана структура матричного перемножувача містить матрицю однорозрядних повних суматорів з парафазними входами та виходами, що дозволило реалізувати інформаційні переноси

між суматорами з гранично мінімальною затримкою сигналів на 1 мікротакт, а крім того підвищити регулярність структури матриці суматорів, що спрощує проектування та нарощення розрядності утилітів таких багаторозрядних пристроїв на реконфігурованих програмних кристалах ПЛІС.

Недоліком такого матричного перемножувача є велика структурна складність, яка обумовлена тим, що матриця однорозрядних суматорів пристрою містить структурно складні повні однорозрядні суматори з парафазними входами та виходами [10], що приводить до значної кількості інформаційних зв'язків між утилітами мікроелектронного кристала матричного перемножувача.

Іншим недоліком такого перемножувача є застосування у його структурі апаратно складних повних однорозрядних суматорів з парафазними входами та виходами, які містять 20 – логічних елементів [10].

Крім того, недоліком такого матричного перемножувача є обмежені функціональні можливості, які обумовлені тим, що його структура не містить вхідного та вихідного регістрів пам'яті, що не дозволяє використовувати його у якості компонента розпаралеленого синхронізованого формування та зчитування цифрових добутків двійкових чисел, наприклад, у цифрових кореляторах, цифрових фільтрах та процесорах шифрування даних з глибоким розпаралеленням обчислювальних операцій.

Матричний перемножувач (рис.6) [11], який характеризується розширеними функціональними можливостями шляхом введення вхідного та вихідного регістрів пам'яті, містить вхідну шину двійкових кодів перемножуваних чисел X та Y (1) , вхідний регістр пам'яті на D-тригерах з парафазними виходами (2), перемножувальну матрицю (4) на основі однорозрядних повних двійкових суматорів з парафазними входами та виходами, вихідний регістр пам'яті з пара фазними виходами добутків перемножуваних чисел (5) та входи синхронізації запису даних (3, 6) у регістри пам'яті.

Зменшення структурної та апаратної складності, розширення функціональних можливостей матричних перемножувачів без зменшення швидкодії здійснено у запропонованому матричному перемножувачі шляхом застосування у матриці суматорів пристрою однорозрядних неповних та повних суматорів з прямими входами та виходами сум та інверсними виходами наскрізних переносів.

На рис.7 показана структурна схема запропонованого удосконаленого матричного перемножувача, який містить 1 – вхідну шину двійкових кодів перемножуваних чисел; 2 – перший регістр пам'яті; 3 – перший синхронізуючий вхід пристрою; 4 – матрицю однорозрядних суматорів (рис.8) на основі удосконаленого однорозрядного неповного суматора (рис.9а), однорозрядного повного суматора з прямим входом та інверсним виходом переносів (рис. 9б), повного однорозрядного суматора з інверсними входами та виходом переносу (рис. 9в) [12], повного однорозрядного суматора з інверсним входом переносу та прямим виходом переносу (рис. 9г); 5 – другий регістр пам'яті; 6 – другий синхронізуючий вхід пристрою.

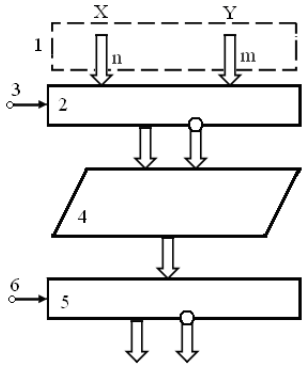


Рис.6. Структурна схема матричного перемножувача

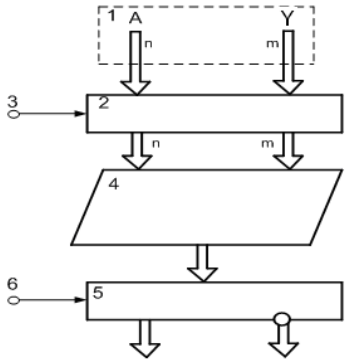


Рис.7. Структурна схема запропонованого матричного перемножувача

На рис.8 приведена структурна схема матриці суматорів пристрою.

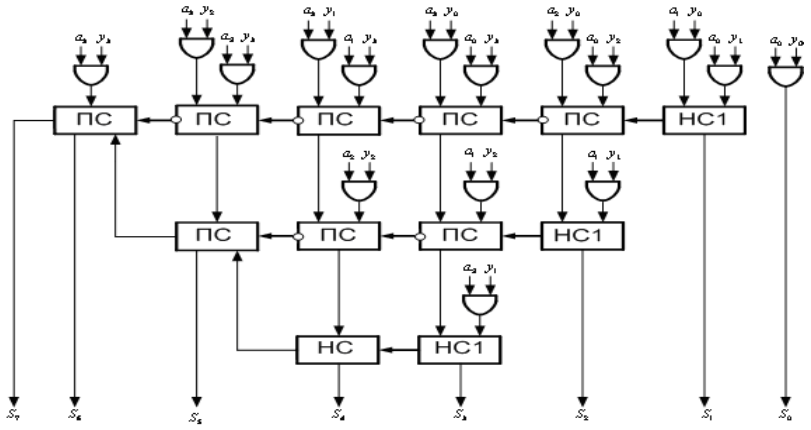


Рис.8. Структурна схема матриці суматорів

У результаті введення у структуру пристрою однорозрядних повних та неповних суматорів з інверсними виходами та входами переносів забезпечується висока швидкодія багаторозрядного матричного перемножувача із затримкою сигналів у горизонтальних інформаційних зв'язках на 1 мікротакт.

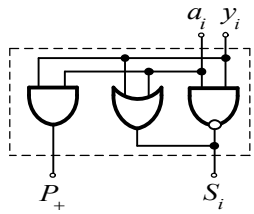
Оцінка структурної складності відомого пристрою розраховується згідно виразу:

$$k_{cП1} = 4\text{n} \cdot k_{c1} + k_{c2}$$

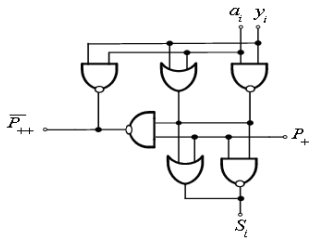
де, k_{c1} – структурна складність тригерів; k_{c2} – структурна складність матриці суматорів, n – розрядність суматора, де

$$k_{c2} = (n^2 - n) \cdot (k_{cПС} + k_{cZв} + k_{cZз}) + 4\text{n} \cdot \text{k}_{\text{сш}} + k_{cЛЕ},$$

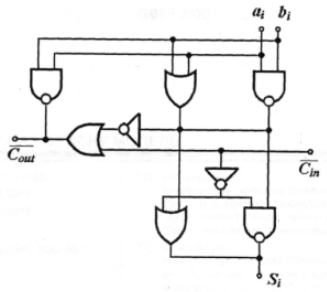
де $k_{cПС}$ – структурна складність повного однорозрядного суматора з парафазними входами і виходами; $k_{cЛЕ}$ – структурна складність логічного елемента "І"; k_{cz3} – структурна складність зовнішніх інформаційних зв'язків, $\text{k}_{\text{сш}}$ – структурна складність вхідної та вихідної шин.



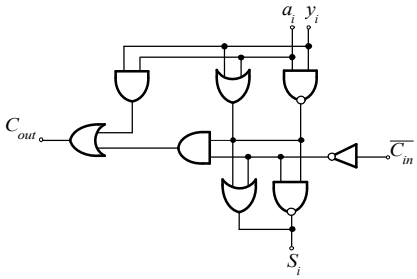
а) Неповний однорозрядний суматор
з прямими входами і виходами



б) Повний однорозрядний суматор
з прямими входами та інверсним виходом



в) Повний однорозрядний суматор
з інверсними входами та виходом переносу



г) Повний однорозрядний суматор з інверсним входом
переносу та прямим виходом переносу

Рис. 9. Компоненти перемножуваної матриці

$$K_{СП1} = 4\text{n} \cdot K_{С1} + ((n^2 - n) \cdot (K_{СПС} + K_{СZз}) + 4\text{n} \cdot \text{k}_{\text{сш}} + K_{СЛЕ}) =$$
$$= 4\text{n} \cdot 30 + ((n^2 - n) \cdot (1057,4 + 12) + 4 \cdot \text{n} + 11,2).$$

Структурна складність удосконаленого матричного перемножувача визначається згідно виразу:

$$k_{сП2} = 4\text{n} \cdot k_{с1} + k_{с2},$$

де

$$k_{с2} = ((\text{n}^2 - 2n) \cdot (k_{сПС} + k_{сzз}) + n \cdot (k_{сНС} + k_{сzз})) + 4n \cdot k_{сш} + \text{n}^2 \cdot (\text{k}_{\text{сЛЕ}} + k_{сzз}) =$$
$$= ((\text{n}^2 - 2n) \cdot (175 + 4) + n \cdot (115,2 + 4)) + 4n + \text{n}^2 \cdot (11,2 + 3),$$

де $k_{сНС}$ – структурна складність напівсуматорів; $k_{сПС}$ - структурна складність повних суматорів.

$$k_{сП2} = 4n \cdot k_{с1} + ((\text{n}^2 - 2n) \cdot (k_{сПС} + k_{сzз}) + n \cdot (k_{сНС} + k_{сzз})) + 4n \cdot k_{сш} + \text{n}^2 \cdot (\text{k}_{\text{сЛЕ}} + k_{сzз}) =$$
$$= 4\text{n} \cdot 30 + ((\text{n}^2 - 2n) \cdot (175 + 4) + n \cdot (115,2 + 4)) + 4n + \text{n}^2 \cdot (11,2 + 3).$$

Швидкодія матричного перемножувача, структура якого показана на рис.7 визначається затримкою сигналів у тригерах вхідного та вихідного регістрів пам'яті (2υ – мікротакти) та затримкою сигналів у перемножувальній матриці ($(2n-1) \cdot \tau_{ПС}$), ($\tau_{ПС} = 2\upsilon$). Тобто, затримка сигналів у регістрах пам'яті не залежить від розрядності перемножуваних чисел і складає 2 мікротакти, а затримка сигналів у перемножувальній матриці визначається згідно виразу ($(2n-1) \cdot \tau_{ПС}$). Тобто при розрядності перемножувача у діапазоні ($128 \div 2048$ біт) відповідно змінюється часова складність матриці перемножування у діапазоні ($(2 \cdot (128 \div 2048) - 1) \cdot 2 = 510 \div 8190$) $510 \div 8190\upsilon$.

В результаті проведених досліджень отримано порівняльну діаграму структурної складності удосконаленого матричного перемножувала відносно відомого [8] у залежності від розрядності перемножуваних двійкових чисел (4-128) (рис.10).

Діаграма залежності швидкодії матричного перемножувача від розрядності перемножуваних чисел приведена на рис.11.

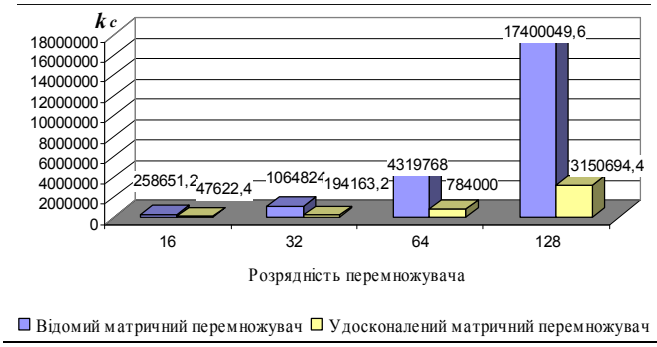


Рис.10. Порівняльна діаграма структурної складності матричних перемножувачів

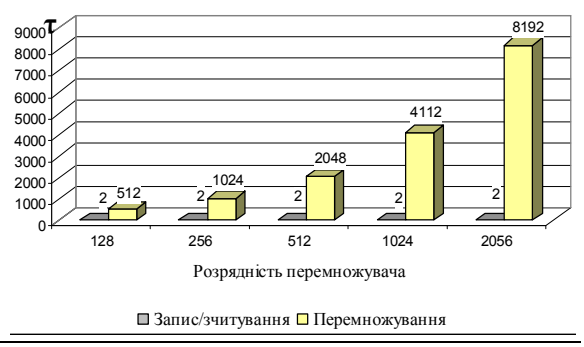


Рис.11. Графік зміни часової складності перемножувача в залежності від розрядності перемножуваних двійкових чисел

4 Потоковий перемножувач

Перемножувачі двійкових чисел є важливими компонентами арифметико-логічних пристроїв універсальних та спеціалізованих процесорів. При значній розрядності множників 32-512 біт такі перемножувачі застосовуються в універсальних комп'ютерах у якості швидкодіючих співпроцесорів. У сучасній обчислювальній техніці найширше застосування отримали матричні перемножувачі з паралельним вводом та виводом даних, що суттєво знижує ефективність їх використання у якості потокових перемножувачів, які є базовими компонентами мультиядерних та систолічних процесорів [6]. Особливо негативно цей недолік проявляється при опрацюванні багаторозрядних двійкових кодів (1024÷4096 біт) процесорами шифрування даних. Крім того є практично

недоцільним реалізація чіпів перемножувачів з вказаним числом виводів. Перспективним напрямком вирішення цієї проблеми є створення потокових перемножувачів з високим рівнем розпаралелення обчислювальних операцій та біт-орієнтованою організацією вводу та виводу даних. Наявність великої кількості входо-виходів ($4n$) у таких багаторозрядних перемножувачах приводить до значного збільшення структурної складності їх вхідних та вихідних шин. Це приводить до відповідного зростання габаритів чіпів, збільшення кількості зовнішніх клем приєднань та зв'язків між кристалом та вихідними клемами з'єднань.

Запропоновано новий потоковий алгоритм виконання операції множення і структура потокового перемножувача [8], яка показана на рис.12.

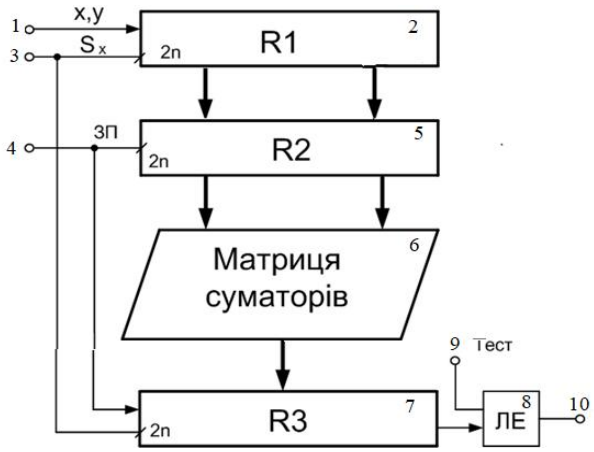


Рис.12. Структура потокового перемножувача двійкових чисел

Принцип роботи потокового перемножувача полягає у розпаралеленні процесів запису, перемноження та зчитування даних. При цьому затримка сигналів у вхідному та вихідному регістрах пам'яті пристрою ($(2n \cdot \tau_T) + \tau_T$), $\tau_T = 2$. Тобто при зміні розрядності потокового перемножувача у діапазоні ($128 \div 2048$ біт), часова затримка сигналів у регістрах вводу-виводу відповідно складає ($2 \cdot (128 \div 2048) \cdot 2 = 512 \div 8192$) $512 \div 8192\upsilon$, що показано на рис.13.

Представлені на діаграмі результати порівняння матричного та потокового перемножувача показують, що затримка сигналів у потоковому перемножувачі на 3 мікротакти (з врахуванням затримки сигналів на 1 мікротакт у вихідному логічному елементі "Виключаюче АБО") перевищує затримку сигналів відомого матричного перемножувача, не залежно від розрядності перемножуваних двійкових чисел.

Структурна складність потокового перемножувача визначається згідно виразу:

$$k_{cПП} = 6\mathrm{n} \cdot k_{c1} + k_{c2} + k_{c3},$$

де k_{c2} – структурна складність матриці перемножування

$$k_{c2} = ((\mathrm{n}^2 - 2n) \cdot (k_{cПС} + k_{czз}) + n \cdot (k_{cНС} + k_{czз})) + 4n \cdot k_{cш} + \mathrm{n}^2 \cdot (\mathrm{k}_{\mathrm{cЛЕ}} + k_{czз}) =$$
$$= ((\mathrm{n}^2 - 2n) \cdot (175 + 4) + n \cdot (115{,}2 + 4)) + 4n + \mathrm{n}^2 \cdot (11{,}2 + 3),$$

де $k_{cНС}$ – структурна складність напівсуматорів; $k_{cПС}$ – структурна складність повних суматорів; k_{c3} – структурна складність логічного елемента "Виключаюче АБО".

$$k_{cПП} = 6n \cdot k_{c1} + ((\mathrm{n}^2 - 2n) \cdot (k_{cПС} + k_{czз}) + n \cdot (k_{cНС} + k_{czз})) + 4n \cdot k_{cш} + \mathrm{n}^2 \cdot (\mathrm{k}_{\mathrm{cЛЕ}} + k_{czз}) =$$
$$= 6\mathrm{n} \cdot 30 + ((\mathrm{n}^2 - 2n) \cdot (175 + 4) + n \cdot (115{,}2 + 4)) + 4n + \mathrm{n}^2 \cdot (11{,}2 + 3) + 68.$$

В результаті проведених досліджень отримано порівняльну діаграму структурної складності потокового перемножувача у залежності від розрядності перемножуваних чисел (рис.14).

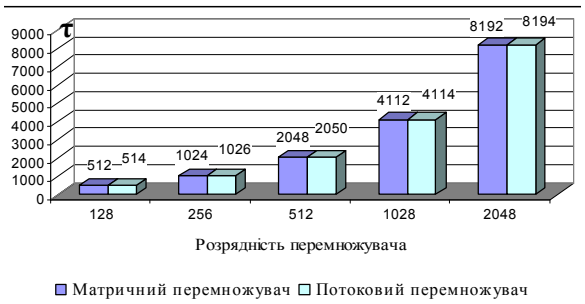


Рис.13. Порівняльна діаграма часової затримки сигналів у матричному та запропонованому потоковому перемножувачах

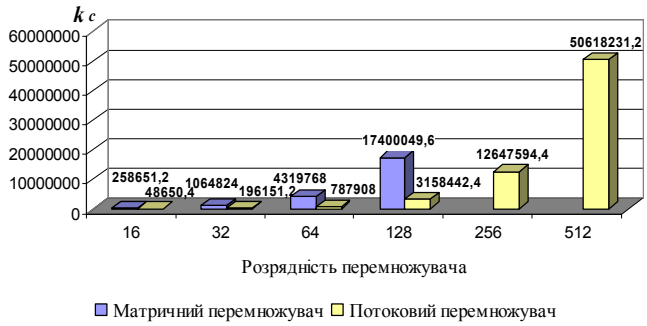


Рис.14. Діаграма зміни структурної складності потокового перемножувача в залежності від розрядності перемножуваних двійкових чисел

У запропонованому потоковому переможувачі досягнута гранично мінімальна структурна складність вхідної та вихідної шин. Тобто структурна складність цього компонента потокового перемножувача зменшена у $4n/2$ разів, що при розрядності вхідних чисел 512, 1024, 2048 згідно критерію Квайна складає 1024, 2048 та 4096 разів.

У загальному випадку зменшення структурної складності входо-виходів мікроелектронних чіпів потокового перемножувача у порівнянні з матричним перемножувачем складає $4n/5$, тобто при розрядності вхідних чисел 512, 1024, 2048 згідно критерію Квайна складає 409,6, 819,2, 1638,4 разів.

Внаслідок застосування у запропонованому потоковому перемножувачі удосконалених структур однорозрядних неповних та повних суматорів на основі логічного елемента "Виключаюче І" з максимальною апаратною складністю 8 вентилів, у порівнянні з відомими структурами, досягнуто зменшення у 2,5 рази апаратної складності перемножуваної матриці, яка містить однорозрядні суматори з парафазними входами та виходами (20 вентилів).

Крім того, розроблений потоковий перемножувач характеризується розширеними поліфункціональними можливостями, оскільки дозволяє виконувати діагностування правильності операції множення шляхом порівняння вихідних кодів добутків з заданим кодом добутку двох відомих багаторозрядних перемножуваних чисел. Шифрування та криптозахист вихідних кодів потокового перемножувача реалізується шляхом модульного біт-орієнтованого додавання вихідних кодів добутків з 2^n-розрядною псевдовипадковою послідовністю, яка поступає на другий вхід вихідного логічного елемента "Виключаюче АБО".

В частковому випадку, коли два перемножувані двійкові числа однакові, пристрій реалізує операцію піднесення до квадрату, а коли одне з чисел рівне 1 – на виході формується криптозахищений код іншого числа.

Розроблені потокові перемножувачі з біт-орієнтованим вводом та виводом цифрових даних можуть бути ефективно застосовані у якості швидкодіючих малогабаритних кристалів у структурах процесорів крипто захисту потоків даних та інших алгоритмах опрацювання двійкових чисел з розрядністю 1024-2048 біт.

Висновки

Запропоновані структурні рішення елементів та функціональних компонентів складних розподілених та кіберфізичних КС. Удосконалена структура перемножувача унітарних кодів у базисі Хаара-Крестенсона, які представляють діапазон квантування кольорів RGB-пікселів у діапазоні амплітуд $0 \div 256$ рівнів дає змогу підвищити швидкодію більш, ніж на 1 порядок, а також досягти більш високої регулярності мікроелектронної структури.

Запропонована структура різницево-модульного квадратора дозволила підвищити швидкодію обчислень модульних різниць квадратів більше, ніж на 1 порядок. При діапазоні кодування вхідних чисел $N = 255$, що відповідає кількості рівнів квантування окремих кольорів RGB-пікселів,

пристрій дозволяє реалізувати визначення Хеммінгової віддалі між пікселями кожного з кольорів зображень. При накопиченні кодів отриманих окремих різницевих квадратів, згідно матриці пікселів відеозображення, реалізується можливість розпізнавання двох зображень на основі інтегральної оцінки Хеммінгової віддалі у квадратичному Евклідовому просторі.

Структура матричного перемножувача двійкових чисел, у якому застосовані удосконалені структури одноразрядних неповних та повних суматорів, дозволила без зменшення швидкодії пристрою зменшити його структурну складність, більше, ніж у 5 разів, а апаратну складність зменшити у 2,5 рази.

У структурі потокового перемножувача досягнуто розширення його функціональних можливостей шляхом застосування на вихідній шині логічного елемента "Виключаюче АБО", який дає змогу здійснити перевірку достовірності результатів множення та криптозахист вихідних кодів реалізацією операції $\oplus$ з біт-орієнтованою багаторозрядною кодовою послідовністю;

Список літератури

1. Vozna N.Ya. Strukturizaciia polifunkcionalnyh danyh: teoriya, metody ta zasoby: monografia / N.Ya.Vozna – Ternopil: TNEU, 2018. – 378 s.

2. Baciuk T.M. Metody ta zasoby multimediynih informaciynih sistem: navch. posibhyk / T.M.Baciuk, P.I.Gegnich. – Lviv: Vidavnictvo Lvivskoi politekhniky, 2015. – 428 s.

3. Pat.107811 Ukraina Chisloimpulsniy mnojilniy pristriy, Bul. №12/2016.

4. Nikolaichyk Ya.N. Chisloimpulsnoe mnojilnoe ustroistvo // A.C. SSSR № 754414. – Bul. № 29. – 1980.

5. Pat.132145 Ukraina Riznicevo-modulniy kvadrator, Bul. №3/2019.

6. Melnyk A.O. Arkhitektura komputera. / A.O.Melnyk – Lutck: Volinska oblasna drukarnia, 2008. – 470 s.

7. Tsilker B.Ya. Organizacia EVM i system: uchebnik dlia vuzov / B.Ya.Tsilker, S.A.Orlov – SPb.: Piter, 2006. – 668 s.

8. Visokoproduktivni matrichni ta potokovi peremnoguvachi tsifrovikh danyh / Ya.M.Nikolaychyk , N.Ya.Vozna V.M.Griga [ta in.] // Matematichne ta kompiyterne modeliuvannia: Tekhnichni nauki: zbirnik naukovykh prats. Kamianets-Podilskyi: Kamianets-Podilskyi nicionalniy universitet im.I.Ogienka, 2019. – Vip.19. – S.101-107. DOI: 10.32626/2308-5916.2019-19.101-107

9. Pat.123752 Ukraina Peremnoguvach potokiv bagatorozriadnikh danikh, Bul. № 21/2021.

10. Pat.109136 Ukraina Odnorozriadniy sumator, Bul. №15/2016.

11. Pat. 132520 Ukraina Matrichniy peremnoguvach, Bul. №4/2019.

12. Pat. 124563 Ukraina Povniy odnorozriadniy sumator, Bul. №7/2018.

IMPROVEMENT OF MULTI-DIGITAL MULTIPLICATING DEVICES STRUCTURES IN DIFFERENT THEORETICAL AND NUMERICAL BASES

[1]Nataliia Vozna, [1]Alina Davletova, [1]Yaroslav Nykolaychuk, [2]Volodymyr Gryga

[1]Western Ukrainian National University, Deparlament of Specialized Computer System
[2]V. Stefanyk Precarpathian National University, Department of Computer Engineering and Electronics

The article proposes methods for improving the structures of multi-bit multipliers, which are characterized by increased speed, reduced structural complexity of the device and reduced structural complexity of inputs and outputs depending on the bit multipliers (512-2048 bits), respectively (1024-4096) times, compared with known multipliers based on classic single-digit full adders. Optimization of structures of multi-bit multipliers is offered. Comparative estimates of structural, functional and relative functional and structural complexities of their circuit implementations are given. The use of optimized circuit solutions of multipliers allows to significantly improve the system characteristics of complex computing devices with a large number of such components in the crystals of microelectronic technologies.

Keywords: multi-bit multipliers, structural complexity, improvement of structures.