УДК 681.32

***Николайчук Я.М.* [1], *Івасьєв С.В.* [1], *Посвятовська О.Б.* [2], *Томчишин О.Б.* [3]**

[1]*Тернопільський національний економічний університет*

[2]*Галицький коледж ім. В. Чорновола*

[3]*Теребовлянський НВК*

ПРИСТРІЙ ФАКТОРИЗАЦІЇ БАГАТОРОЗРЯДНИХ ЧИСЕЛ

Вступ. Обчислювальна складність методу факторизації Ферма для багато розрядних чисел (БРЧ) експоненційна. Із збільшенням розрядності вона відповідно зростає, оскільки число процесів k може складати 2^{300} - 2^{400} і тільки на єдино правильному кроці можливе однозначне рішення задачі факторизації. Слід зазначити, що при використанні методу факторизації необхідно підносити до квадрату числа з розрядністю 300-500 біт, що приводить до необхідності кожного разу знаходити різницю та добувати корені квадратні з цієї різниці.

Мета: Дослідження та розробка високоефективного пристрою факторизації багаторозрядних простих чисел.

1. Дослідження існуючих аналогів пристрою для факторизації багаторозрядних чисел

Робота існуючих аналогів пристрою полягає у тому, що число m представляється k-розрядним двійковим числом, з якого визначається ціла частина від квадратного кореня з n, $m = \lfloor \sqrt{n} \rfloor$ для різних значень *x=1,2,…,* послідовно багатократно визначається значення згідно виразу $q(x) = (m + x)^2 - n$ до тих пір, поки отримане значення не буде рівне повному квадрату у вигляді цілого числа згідно двійкової арифметики. Недоліком такого алгоритму є велика обчислювальна складність, яка обумовлена виконанням великого числа обчислювально-складних операцій у позиційній двійковій системі числення над БРЧ, які включають операції піднесення до степеня, додавання, віднімання та добування квадратного кореня числа, розрядність якого експоненційно зростає, починаючи з розрядності числа n. Недоліком також є низька швидкодія реалізації способу факторизації БРЧ, обумовлена наявністю наскрізних переносів при виконанні операцій додавання, множення, піднесення до квадрату та віднімання, які в найбільшій мірі знижують швидкодію реалізації способу факторизації БРЧ [1].

Розглянемо приклад факторизації БРЧ у двійковій системі числення над десятковими числами, заданими у прикладі:
n = 10001010111111000110001011111000100101000100101100001000101010 101111000 1010101011101011101010001000101 (k=102). Для визначення 51-розрядних двійкових чисел p=10001100000101000001111011010011101 1101010110000111 та q=11111100000000011000110000100111111111 01011010011 необхідно виконати операцію визначення кореня квадратного $m = \lfloor \sqrt{n} \rfloor$ = 10111100101000001010110100000101010101110011100000, визначити цілу частину 101111001010000010101101000001010 10 1011110011100000 та виконати x=1000011010011100010101101110100 0010101101001100 ітерацій для визначення числа q(x). На завершальному кроці ітерації отримується число $(m + x)^2 - n =$

10010111101010010001010010010011011101100110001100100000101101110011011111 0
00011011111110001111001000 0 .

2. Розробка пристрою для факторизації багаторозрядних чисел

Поставлена задача розробки ефективного пристрою факторизації БРЧ у системі числення залишкових класів ТЧБ Крестенсона, дозволяє зменшити обчислювальну складність та підвищити швидкодію процесу факторизації шляхом вилучення операцій добування квадратного кореня при виконанні багатократних ітерацій[2], а також зменшити розрядність чисел, над якими виконуються обчислювальні операції. Це приводить до підвищення швидкодії реалізації способу факторизації БРЧ у порівнянні з відомим способом на два-три порядки, оскільки операції віднімання, множення та піднесення до степеня виконуються паралельним способом без наскрізних переносів згідно арифметики системи числення залишкових класів ТЧБ Крестенсона [3].

Розроблений пристрій працює наступним чином: з відомого числа *n*, представленого в двійковій системі числення, визначається корінь квадратний, який округлюється до більшого цілого у вигляді P_c^*.

Отримане число представляється залишками $b_1,b_2,b_i,\ldots,b_k]$, $i=1,2,3...k$ у системі взаємно простих модулів $[p_1,p_2,p_i,\ldots,p_k]$ згідно виразу $b_i = \text{res } P_c^* \bmod p_i$. Визначається квадрат $S_0 = (P_c^*)^2 = (S_1,S_2,S_i,S_k)$, $i=1,2,3...k$ згідно модульної арифметики СЗК $S_i = \text{res } (b_i \times b_i) \bmod p_i$, додатково визначається різниця між значеннями $\Delta_0 = S_0 - n$ згідно модульної арифметики СЗК $\Delta_{0i} = \text{res } S_{0i} - b_i$, визначається крок приростів квадратів, починаючи з S_0 згідно виразу $2 \cdot P_c^* + 1$, ітераційно виконується визначення значень S_x у модульній арифметиці СЗК згідно виразу $S_x = 2 \cdot P_c^* x + x^2 + \Delta_0$.

Запам'ятовуються у стекову пам'ять отримані значення S_x, S_{x-1}, S_{x-2} ,…,S_{x-z}, записуються у стекову пам'ять $P_c^* + x$, які є коренями квадратними з S_x , у кожній ітерації порівнюються значення S_x з усіма значеннями S_{x-z}, які містяться у стековій памяті, а при співпаданні кодів $S_{x.i} = S_{x-z,i}$ у СЗК факторизовано числа *p*,*q* визначаються згідно виразів $p = P_c^* + x - \sqrt{S_{x-z,i}}$, $q = \sqrt{S_{x-z,i}} + P_c^* + x$ представлених в [4].

Розглянемо простий приклад. Нехай $n=93=pq$, де $p=3$, $q=31$. На рисунку 4.25 показано граф розв'язання запропонованого способу реалізації, де $\sqrt{n} \approx 9{,}6436507$, тобто наближення до більшого цілого $\lfloor \sqrt{n} \rfloor = 10$, таким чином найближчий старший квадрат $10^2 = 100$, звідки $\Delta_0 = 100 - 93 = 7$, таким чином стартове значення $S_0 = 7$, а крок зростання квадратів дорівнює $2 \cdot 10 + 1 = 21$, наступні кроки збільшуються на 2. Запам'ятовуються стартовий корінь квадратний та його квадрат, який відповідно на кожній ітерації буде змінюватися з кроком 21, 23, 2 5,… в стековій пам'яті, на кожній ітерації відбувається асоціативне порівняння чисел в СЗК S_x з поточними квадратами, що містяться у асоціативній стековій пам'яті.

Розглянемо виконання процесу факторизації числа n на прикладі кодів СЗК. Вибираємо систему взаємно простих модулів залишкових класів, розрядність добутку яких перевищує розрядність *n*(рисунок 1).

При співпадінні отриманого значення із значенням, що у стековій пам'яті, завершується процес факторизації числа *n,* як показано стрілкою на рисунку 4.25.

Нехай $p_1=5$, $p_2=7$, $p_3=11$ - обрана система взаємно простих модулів. Розрядність добутку обраних модулів (8 біт) задовільняє умові і перевищує розрядність *n=93.*

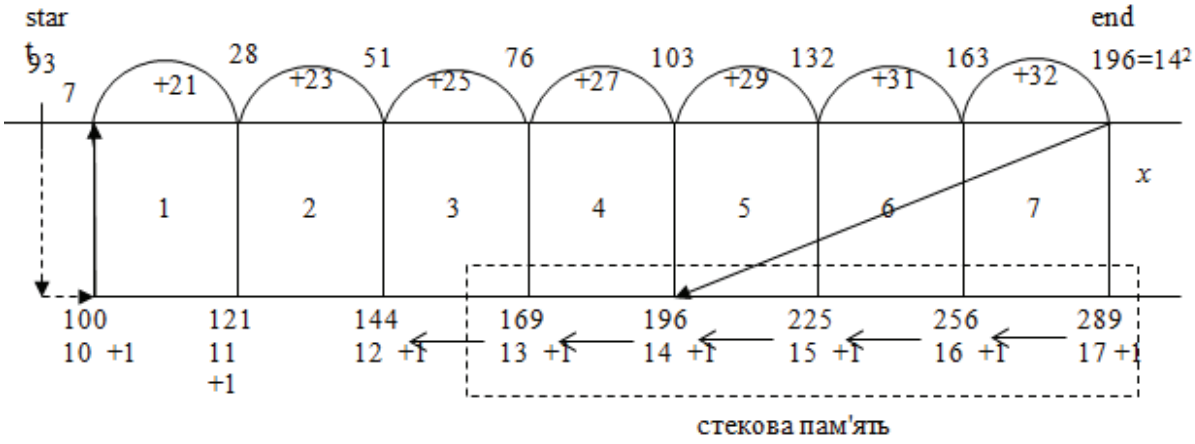

Рисунок 1 - Процес факторизації n – розрядного числа

Представляємо Δ_0 в системі залишкових класів:

$$\Delta_0=7 \begin{cases} \text{res (mod 5)} = 2; \\ \text{res (mod 7)} = 0; \\ \text{res (mod 11)} = 7; \end{cases} \qquad 2 \cdot P_z^* + 1 = 21 \begin{cases} \text{res (mod 5)} = 1; \\ \text{res (mod 7)} = 0; \\ \text{res(mod 11)} = 10; \end{cases}$$

$$10 \begin{cases} \text{res (mod 5)} = 0; \\ \text{res (mod 7)} = 3; \\ \text{res (mod 11)} = 10; \end{cases} \qquad 100 \begin{cases} \text{res (mod 5)} = 0; \\ \text{res (mod 7)} = 2; \\ \text{res (mod 11)} = 1. \end{cases}$$

Виконуємо операції запропонованого способу факторизації, використовуючи обрану систему взаємно простих модулів ($p_1=5$, $p_2=7$, $p_3=11$) у СЗК, як показано в таблиці 1.

Таблиця 1 - Метод факторизації використанням системи взаємно простих модулів($p_1=5$, $p_2=7$, $p_3=11$)

x	0	1	2	3	4	5	6	7
$P_1=5$	2	3	1	1	3	2	3	1
	1	3	3	0	2	4	1	2
	0	1	2	3	4	0	1	2
	0	1	4	4	1	0	1	4
$P_2=7$	0	0	2	6	5	6	2	0
	0	2	2	4	6	1	3	4
	3	4	5	6	0	1	2	3
	2	2	4	1	0	1	4	2
$P_3=11$	7	6	7	10	4	0	9	9
	10	1	1	3	5	7	9	10
	10	0	1	2	3	4	5	6
	1	0	1	4	9	5	3	3
	7	28	51	76	103	132	163	196
	21	23	23	25	27	29	31	17
	10	11	12	13	14	15	16	17
	100	121	144	169	196	225	256	289

Уведення виконання операції факторизації БРЧ на основі представлення чисел у системі числення залишкових класів дозволяє на 3 - 4 порядки підвищити швидкодію реалізації способу за рахунок виконання модульних операцій піднесення до квадрату, множення, додавання та порівняння на основі модульної арифметики, які виконуються паралельно по кожному модулю за 2 - 4 мікротакти, оскільки не містять наскрізних переносів і їх швидкодія не залежить від розрядності чисел, які факторизуються.

Функціональна схема пристрою наведена на рисунку 2.

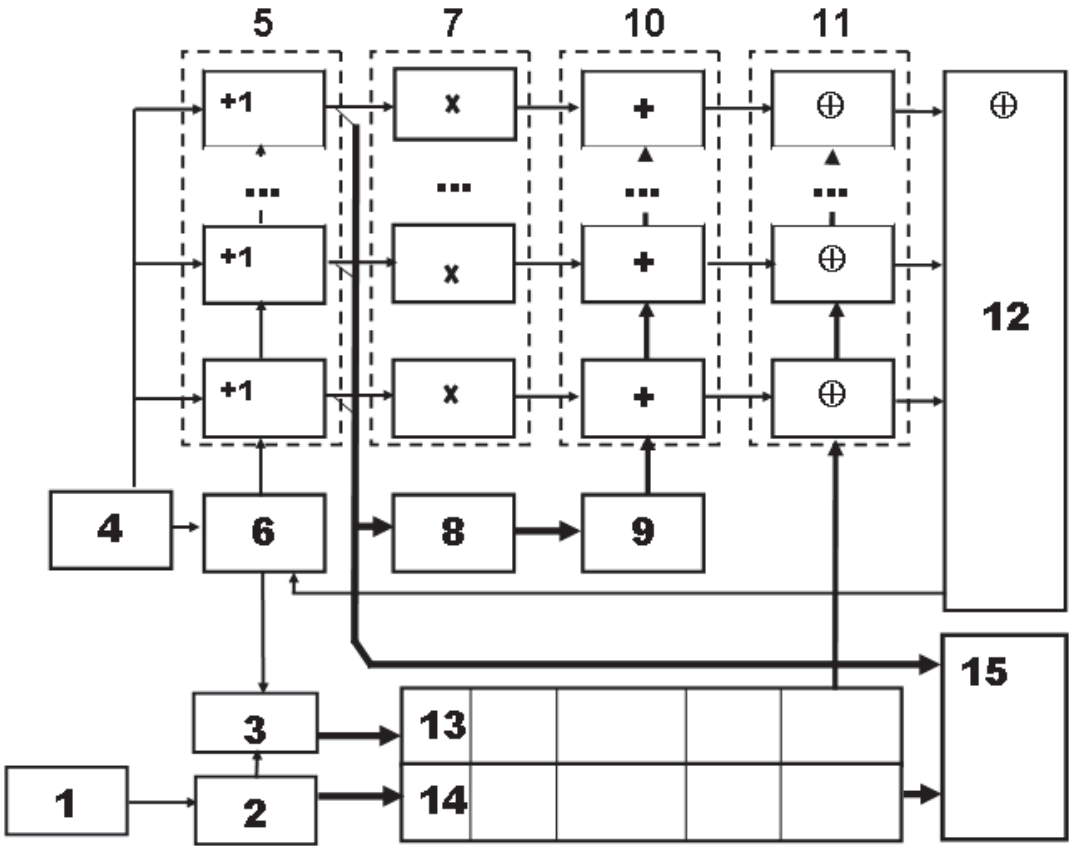

Рисунок 2 – Схема реалізації способу факторизації в СЗК

Пристрій складається з таких компонентів: 1 – блок вводу двійкового коду числа, що факторизується; 2 - блок визначення двійкового значення квадратного кореня числа n з заокругленням до більшого цілого, перетворення його у СЗК та ітераційного формування інкрементно зростаючих кодів; 3 - блок здійснює модульне піднесення числа у системі числення залишкових класів до квадрату та формування їх інкрементної послідовності у кожному циклі ітерації; 4 – стартовий блок початку процесу факторизації; 5 – лічильник у базисі Хаара-Крестенсона; 6 - тактовий генератор; 7 - блок формування кодів квадратів числа ітерацій у СЗК; 8 - блок перемноження; 9 - перший блок додавання; 10 - другий блок додавання; 11 - блок порівняння кодів; 12 - блок визначення рівності кодів; 13 - стекова пам'ять асоціативна квадратів; 14 – стекова пам'ять коренів квадратних квадратів у двійковій системі числення; 15 - блок реєстрації та перетворення кодів СЗК у двійкову систему числення.

Досягнуте підвищення швидкодії запропонованого способу факторизації [5] дозволяє спростити розв'язання ряду фундаментальних задач теорії чисел, зокрема: розкладу числа на прості множники, визначення символів Якобі, генерація БРПЧ,

повний розклад числа на множники [6-7].

Процес факторизації згідно запропонованого способу включає наступні етапи: число, що факторизується, з блоку 1 поступає на вхід блоку 2, який здійснює у двійковій системі числення визначення кореня квадратного, округлюється до більшого цілого, перетворюється в СЗК і з першого виходу поступає в стекову пам'ять 14, на виході якої у блоці 15 формується двійковий код завершення процесу факторизації. В блоці 3 здійснюється формування квадратів чисел у СЗК, що записуються у асоціативну стекову пам'ять 13.

Початок процесу факторизації здійснює блок 4, який записує стартовий код числа ітерацій в блок 5 та виконує запуск тактового генератора 6, під дією тактових сигналів генератора 6 здійснюється інкрементне формування та запис інкрементно наростаючих кодів СЗК у стекову асоціативну пам'ять 13, 14, а також інкрементне кодування числа ітерацій у блоці 5 та їх реєстрація у блоці 15. При цьому синхронно у блоці 7 виконується піднесення числа ітерацій до квадрату, а у блоці 8 - перемноження числа ітерацій на постійний код $2P_c$. В блоці 9 відбувається додавання отриманих результатів з кодом Δ_0.

Далі отримана сума додається до квадратів чисел, які формуються у блоці 10. В 11 відбувається порівняння отриманої суми блоку 10 з усіма кодами асоціативної пам'яті 13 і у випадку співпадіння одного з кодів, що визначається блоком 12, вихідний сигнал, якого зупиняє тактовий генератор 6. При цьому на виході 15 реєструються коди числа ітерацій та кореня квадратного асоціативної пам'яті 14, що є завершенням процесу факторизації. Код реалізації пристрою для факторизації багаторозрядного числа на ПЛІС наведений в додатку Н, а його технологічна схема - в додатку П.

Основна апаратна складність спецпроцесора факторизації розраховується згідно схеми, представленої на рисунку 4.26, складається з суми апаратної складності його компонентів:

$A_5+A_6+A_7+A_8+A_9+A_{10}+A_{11}+A_{12}+A_{13}+A_{14}+A_{15}$.

Розрахунок виконано для 32-бітного спецпроцесора:

$A_5=(P_1+P_2+P_3+P_4+P_5+P_6+P_7)2=(17+19+23+25+27+29+31)2=257\ v;$

$A_6=4v$;

$A_7=(P_1+P_2+P_3+P_4+P_5+P_6+P_7)/2=(17+19+23+25+27+29+31)/2=86\ v;$

$A_8=(P_1+P_2+P_3+P_4+P_5+P_6+P_7)=171;$

$A_9=(P_1+P_2+P_3+P_4+P_5+P_6+P_7)=171;$

$A_{10}=(P_1^2+P_2^2+P_3^2+P_4^2+P_5^2+P_6^2+P_7^2)+(P_1+P_2+P_3+P_4+P_5+P_6+P_7)=4506\ v;$

$A_{11}=(P_1+P_2+P_3+P_4+P_5+P_6+P_7)\ 320=(17+19+23+25+27+29+31)\ 320=54720\ v;$

$A_{12}=\mathrm{Log}_2(P_1+P_2+P_3+P_4+P_5+P_6+P_7)=8\ v;$

$A_{13}=64\cdot A_7\cdot 2=11008\ v;$

$A_{14}=(16+15+13+11+7)\cdot 2\cdot 64=7936\ v.$

Блоки А1, А4, А15 є інтерфейсними і з'єднані з комп'ютером.

Розрахунок часової складності спецпроцесора факторизації за одну ітерацію роботи алгоритму визначається сумарним числом найбільшого числа послідовно з'єднаних модулів згідно виразу [8-9]:

$$\tau_5+\tau_7+\tau_{10}+\tau_{11}+\tau_{12},\ \text{де}\ \tau_5=2\upsilon;\ \tau_7=1\ \upsilon;\ \tau_{10}=2\upsilon;\ \tau_{11}=3\upsilon;\ \tau_{12}=2\upsilon.$$

Висновок. Тобто число мікротактів виконання однієї ітерації факторизації числа розробленим процесором у базисі Хаара-Крестенсона не перевищує 10 υ. При організації пара-фазних виходів з матрично-модульного суматора 10 швидкодія модуля 11 може бути реалізована за один мікротакт, тому тривалість одного циклу ітерацій буде становити 8υ.

При швидкодії елементої бази ПЛІС $\upsilon = 1$ нс тривалість ітерації не перевищує 10 мікросекунд. За одну годину пристрій виконає приблизно 360000000000 ітерацій. При збільшенні числа розрядів процесора до 512-1024 швидкодія не змінюється за рахунок модульної арифметики. Таким чином, сумарна кількість вентилів 32-бітного спецпроцесора факторизації БРЧ складає 78867 *v*.

Перелік використаних джерел

1. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов.– Казань: Казан. ун. 2011.– 190 с.

2. Івасьєв С.В. Збіжність екстремумів залишкової функції в околі розв'язку задачі факторизації/ С.В.Івасьєв, Я.М. Николайчук, І.З.Якименко, І.Р.Колісник // Вісник Хмельницького національного університету. Технічні науки. – 2015, №4. - С.157-164.

3. Івасьєв С.В. Матричний метод факторизації великорозрядних чисел / С.В. Івасьєв // Поступ в науку. Збірник праць Бучацького інституту менеджменту і аудиту – Бучач. – 2012. - №8. – С. 92-95.

4. Івасьєв С.В. Метод факторизації велико-розрядних чисел в базисі Радемахера / С.В. Івасьєв // Вісник національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів. – 2012. - С. 118–126.

5. Івасьєв С.В. Метод факторизації чисел великої розрядності на основі ТЧБ Радемахера-Крестенсона / С.В. Івасьєв, І.З. Якименко, В.І. Назаров // Сучасні комп'ютерні інформаційні технології: Матеріали V Всеукраїнської школи-семінару молодих вчених і студентів. - 2015. – С.184.

6. Николайчук Я.М. Метод факторизації багаторозрядних чисел та дослідження в околі розв'язання задач / Я.М. Николайчук, С.В. Івасьєв // Матеріали XIV Міжнародного наукового семінару "Сучасні проблеми інформатики в управлінні, економіці та освіті", Київ – оз. Світязь, 29 червня – 3 липня 2015 року. – С.83-88.

7. Николайчук Я.М. Фундаментальні засади теорії факторизації багаторозрядних чисел на основі фракталів зображень в околі рішення / Я.М. Николайчук, С.В. Івасьєв // Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління»(ICSM). – Тернопіль, 2014. – С. 116-120.

8. Ивасьев С.В. Метод факторизации многоразрядных чисел на основе свойств квадратичности вычетов в системе остаточных классов / С.В. Ивасьев, Я.Н. Николайчук, И.З. Якименко, М.Н. Касянчук // Вестник Брестского государственного технического университета. – 2015. – № 5(95): Физика, математика, информатика. – С. 45–45.

9. Тимошенко Л.М. Алгоритми факторизащї для криптоаналізу асиметричних криптосистем / Л.М. Тимошенко, К.В. Вербик, Я.М. Николайчук, С.В. Івасьєв // Інформатика та математичні методи в моделюванні. – Одеса 2014.- № 4(4). – С. 342-349.