Міністерство освіти і науки України
Тернопільський національний економічний університет

ВОЛИНСЬКИЙ ОРЕСТ ІГОРОВИЧ

УДК 681.325

МЕТОДИ ПОБУДОВИ ВИСОКОПРОДУКТИВНИХ СПЕЦПРОЦЕСОРІВ НА ОСНОВІ ТЕОРЕТИКО-ЧИСЛОВОГО БАЗИСУ КРЕСТЕНСОНА

05.13.05 – комп’ютерні системи та компоненти

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2013

Дисертацією є рукопис.

Робота виконана у Тернопільському національному економічному університеті Міністерства освіти і науки України.

Науковий керівник : доктор технічних наук, професор
Николайчук Ярослав Миколайович,
Тернопільський національний економічний університет,
завідувач кафедри спеціалізованих комп'ютерних систем.

Офіційні опоненти:

доктор технічних наук, професор
Мельник Анатолій Олексійович,
Національний університет "Львівська політехніка", завідувач кафедри електронних обчислювальних машин;

доктор технічних наук, професор
Тарасенко Володимир Петрович,
Національний технічний університет України "Київський політехнічний інститут", завідувач кафедри системного програмування і спеціалізованих комп'ютерних систем.

Захист відбудеться 28 листопада 2013 р. о 14^{00} год. на засіданні спеціалізованої вченої ради К.58.082.02 у Тернопільському національному економічному університеті за адресою: 46020, м. Тернопіль, бульв. Т. Шевченка, 9, (корпус 10, конференц-зал).

З дисертацією можна ознайомитися у бібліотеці Тернопільського національного економічного університету за адресою: 46020, м. Тернопіль, вул. Бережанська, 4.

Автореферат розісланий «28» жовтня 2013 р.

Вчений секретар спеціалізованої
вченої ради К.58.082.02 Яцків В.В.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми досліджень. Розвиток теорії універсальних та спеціалізованих процесорів тісно пов’язаний з відповідним розвитком двійкової системи числення, тобто теоретико-числового базису (ТЧБ) Рademахера. Сучасні досягнення у створенні високопродуктивних процесорів пов’язані з розробкою теорії паралельних обчислень, потокової та конвеєрної організації виконання програм, застосування надоперативної та асоціативної багаторівневої пам’яті, а також становлення та розробки теоретичних положень вертикальної інформаційної технології.

Жорсткі зростаючі вимоги до швидкодії процесорів стимулювали дослідження у застосуванні інших, відмінних від базису Рademахера, ТЧБ. Наприклад, відомі успішні застосування базису Крестенсона, математичною основою якого є розширені поля Галуа для побудови високопродуктивних спецпроцесорів системи залишкових класів (СЗК), базису Галуа, який породжує коди поля Галуа та систему числення Галуа, а також, базису Уолша, який використовується при створенні комунікаційних та сигнальних процесорів у комп’ютерних мережах. Однак, в даних дослідженнях мало уваги приділено міжбазисним перетворенням, що особливо актуально при роботі з великорозрядними числами.

Розробка високопродуктивних процесорів опрацювання великорозрядних чисел на основі ТЧБ Крестенсона є актуальною науковою задачею, яка дозволяє вирішити завдання вдосконалення та покращення системних характеристик обчислювальних засобів, як компонентів сучасних розподілених систем, підвищення ефективності захисту інформації в комп’ютерних мережах, а також побудови швидкодіючих спецпроцесорів кореляційного, спектрального та інших застосувань опрацювання інформації.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана в рамках наукових досліджень, що проводились кафедрою спеціалізованих комп’ютерних систем Тернопільського національного економічного університету (м. Тернопіль) по науково-дослідних темах: „Розробка теорії та комп’ютерних засобів спеціалізованих комп’ютерних систем на основі теоретико-числових базисів Крестенсона-Галуа” (державний реєстраційний номер 0106U012530), “Розробка алгоритмів функціонування захистів електропередач за коротких замикань на основі теорії кореляційних функцій” (державний реєстраційний номер 0112U008457), “Розробка теоретичних засад методів формування та цифрового опрацювання даних у розподілених спеціалізованих комп’ютерних системах” (державний реєстраційний номер 0112U008458) та “Методи та засоби побудови безпровідних мультимедійних сенсорних мереж на основі модулярної арифметики” (СКС-04-2013 «Б»).

Мета і задачі дослідження. Метою роботи є розробка високопродуктивних процесорів опрацювання великорозрядних чисел на основі ТЧБ Крестенсона.

Для досягнення поставленої мети необхідно вирішити такі задачі:

1) систематизувати характеристики, проаналізувати сфери застосування процесорів, реалізованих у різних ТЧБ, та дослідити особливості і переваги

машинної арифметики СЗК з метою визначення перспективи застосування перетворень базису Крестенсона для розв’язання задач з великою обчислювальною складністю;

2) дослідити арифметику та форми СЗК і розробити методи приведення СЗК до досконалої форми з метою спрощення часової та апаратної складності процесорів опрацювання великорозрядних чисел;
3) розробити метод виконання операції модулярного множення у розмежованій матрично-модульній системі числення;
4) розробити метод високопродуктивного перетворення чисел з базису Радемахера в базис Крестенсона на основі модулів пам’яті;
5) розробити метод швидкодіючого перетворення чисел з позиційної системи базису Радемахера в систему залишкових класів базису Крестенсона;
6) вдосконалити метод кодування, модульного сумування та множення у теоретико-числовому базисі Хаара-Крестенсона;
7) дослідити алгоритми ділення та модулярного експоненціювання у базисі Крестенсона;
8) розробити апаратні структури та дослідити характеристики компонентів спецпроцесорів у базисі Крестенсона;
9) розробити структурні та принципові рішення спецпроцесорів опрацювання великорозрядних чисел базису Крестенсона;
10) розробити та реалізувати у промисловості програмно-апаратні засоби опрацювання цифрових даних у базисі Крестенсона.

Об’єктом дослідження є процеси цифрового опрацювання великорозрядних чисел високопродуктивними спеціалізованими процесорами у базисі Радемахера-Крестенсона.

Предметом дослідження є методи, способи та засоби опрацювання великорозрядних чисел та міжбазисних перетворень Радемахера-Крестенсона.

Методи дослідження базуються на використанні теорії інформації, теорії чисел та кодування даних, теорії комп’ютерної логіки та теорії цифрового опрацювання даних. Розробка технічних засобів здійснювалась з використанням методів імітаційного моделювання автоматизованого проектування схемо- та системотехніки.

Наукова новизна одержаних результатів полягає в розвитку методів та програмно-апаратних засобів для опрацювання великорозрядних чисел на основі ТЧБ Крестенсона.

Основні результати і положення, що виносяться на захист, спрямовані на створення програмно-апаратних засобів опрацювання цифрових даних у базисі Крестенсона.

Наукова новизна отриманих результатів.

1. Вперше розроблено:

– метод виконання операції модулярного множення у розмежованій матрично-модульній системі числення, який, у порівнянні з відомими, відрізняється тим, що кожен елемент матриці, який відповідає двійковому розряду 2^i, представляється кодом залишку по модулю P, а операція множення виконується шляхом додавання поточних залишків першого

числа з їх подвоєними значеннями по модулю P, які відповідають одиничним елементам коду другого числа, що дозволяє зменшити обчислювальну складність модульних операцій множення та експоненціювання на 2-3 порядки;

- метод перетворення чисел з базису Радемахера в базис Крестенсона рекурентним скануванням двійкових чисел, починаючи зі старшого розряду, що, на відміну від відомих перетворень, шляхом адресної вибірки кодів залишків із модуля пам'яті, виключає операції порівняння та віднімання великорозрядних двійкових чисел з наскрізними переносами і дозволяє підвищити швидкодію міжбазисного перетворення пропорційно розрядності двійкового числа;
- метод швидкодіючого перетворення чисел з позиційної системи базису Радемахера в систему залишкових класів базису Крестенсона, який, на відміну від відомих, шляхом бінарного розмежування, мультиплексування та рандомізації кодів залишків по модулю дозволяє максимально розпаралелити процес визначення кінцевого залишку, швидкодія якого не залежить від розрядності перетворюваних двійкових чисел.

2. Отримав подальший розвиток метод кодування, модульного сумування та множення у теоретико-числовому базисі Хаара-Крестенсона, який відрізняється від відомих представленням цифрових даних у системі взаємопростих модулів базису Крестенсона залишками в кодах базису Хаара, що дозволило замінити обчислювальні операції сумування та множення над двійковими числами матрично-модульними операціями над кодами Хаара і зменшити обчислювальну складність арифметичних операцій на два-три порядки, пропорційно розрядності кодів вхідних даних.

Практичне значення отриманих результатів.

1. Розроблений пристрій визначення залишків багаторозрядного числа, який формує коди залишків розмежованої матрично-модульної системи числення у базисі Радемахера-Крестенсона, який, у порівнянні з відомими аналогами, шляхом заміни великорозрядного двійкового суматора однорозрядним повним суматором та регістрами зсуву, характеризується підвищеною швидкодією та зменшеною апаратною складністю, що розширює його функціональні можливості при опрацюванні великорозрядних чисел у задачах шифрування інформаційних потоків.

2. Розроблено спецпроцесор на основі запропонованого способу визначення залишку двійкового числа шляхом рекурентного сканування великорозрядних чисел базису Радемахера, що у порівнянні з аналогами дозволило підвищити на 2-3 порядки швидкодію визначення залишків чисел по модулю за рахунок застосування модуля пам'яті і виключити наскрізні переноси, які виникають у багаторозрядних суматорах існуючих процесорів.

3. Розроблено високопродуктивний спецпроцесор міжбазисного перетворення Радемахера-Крестенсона, що, у порівнянні з відомими аналогами, шляхом мультиплексування та рандомізації розмежованих залишків дозволило досягнути максимальної швидкодії визначення кодів залишків, у системі взаємопростих модулів, з часовою складністю перемикання двох послідовно

з’єднаних логічних вентилів, незалежно від розрядності перетворюваного двійкового числа.

4. Розроблений швидкодіючий спецпроцесор кореляційного опрацювання сигналів на основі кодування, модульного сумування та множення у теоретико-числовому базисі Хаара-Крестенсона, що дозволило реалізувати однотактні модульні операції додавання та множення на вентильних матрицях і на 2-3 порядки підвищити швидкодію кореляційного опрацювання сигналів у порівнянні з аналогічними процесорами у базисі Радемахера.

Теоретичні та практичні результати роботи використано та впроваджено:

1. В Інституті мікропроцесорних систем керування об’єктами електроенергетики КД ЦІЗІТ НАН України (м.Львів) в інформаційно-діагностувальній системі моніторингу стану ізоляції в електромережах 6-35 кВ на об’єктах ВАТ ЕК «Львівобленерго» (акт від 03.12.2012р.).

2. У Тернопільському конструкторському бюро радіозв’язку «СТРІЛА» при реалізації спецпроцесорів перетворення великорозрядних чисел двійкової системи числення у систему залишкових класів (акт від 30.11.2012р.).

3. На кафедрі спеціалізованих комп’ютерних систем Тернопільського національного економічного університету при викладанні дисциплін: “Комп’ютерна логіка”, “Цифрова обробка сигналів і зображення”, “Теорія джерел інформації”, “Спецпроцесори в різних теоретико-числових базисах” для студентів спеціальностей 8.05010203 - “Спеціалізовані комп’ютерні системи” та 8.05010201 - “Комп’ютерні системи та мережі” (акт від 18.12.2012р.).

Особистий внесок здобувача. Основний зміст роботи, наукові положення та результати сформульовано та вирішено автором самостійно. Внесок здобувача полягає в аналізі сучасного стану рішення науково-технічної задачі, розробці основних ідей, методик досліджень, структурних, принципових та алгоритмічних рішень, організації експериментів, виготовленні дослідного взірця спецпроцесора, а також в розробці необхідного для дослідження програмного забезпечення. У публікаціях, написаних у співавторстві, здобувачеві належить: [3] – запропоновано процедуру розмежування розрядної сітки процесора у базисі Радемахера-Крестенсона; [4] – запропоновано алгоритм порівняння в досконалій системі залишкових класів; [5] – запропоновано застосування розмежованої системи числення для опрацювання великорозрядних чисел; [6] –виконана функціональних можливосте арифметики в базисах Радемахера та Крестенсона; [7] – запропоновано використання матричного перемножувача базису Хаара; [8] – запропоновано структуру пристрою визначення залишку багаторозрядного числа; [9] – запропоновано алгоритм отримання залишку двійкового числа; [10] – запропоновано структурну рандомізатора міжбазисного перетворювача Радемахера-Крестенсона; [11] – запропоновано структуру матрично-модульного перемножувача в базисі Хаара; [12] – проаналізовано структуру модульних шифраторів Радемахера-Крестенсона; [13] – виконано теоретичні дослідження операцій арифметико-логічних у базисі Крестенсона; [16] – запропонований спосіб перевірки подільності чисел на прості модулі; [18] – досліджено пряме перетворення системи залишкових класів; [20] – запропоновано блок-схему алгоритму пошуку залишків великорозрядних чисел Мерсена по простих

модулях; [22] – проаналізовано ТЧБ Радемахера та Крестенсона; [23] – проаналізовано міжбазисні перетворення Радемахера-Крестенсона; [24] – отримано аналітичні вирази оцінки швидкодії виконання арифметичних операцій в базисі Радемахера, Крестенсона та Галуа; [25] – запропоновано блок-схему мультибазисного багатофункціонального спецпроцесора.

Апробація результатів дисертації. Основні результати дисертації доповідались та обговорювались на: міжнародному симпозіумі «Питання оптимізації обчислень» (ПОО - XXXV). – Київ, 2009; 4-ій Міжнародній науково-технічній конференції Advanced Computer Systems and Networks: Design and Application (ACSN). – Львів, 2009; 10-ій міжнародній конференції „Modern problems of radioengineering, telecommunications and computer science ”. – Львів-Славське, 2010; міжнародній проблемно-науковій міжгалузевій конференції «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління». – Бучач-Східниця, 2010; XIth International conference“The experience of designing and application of CAD systems in micro-electronics. – Lviv, 2011; міжнародній молодіжній математичній школі “Питання оптимізації обчислень (ПОО-XXXVII)” – Київ, 2011; проблемно-науковій міжгалузевій конференції «Юриспруденція та проблеми інформаційного суспільства» (ЮПІС - 2011), - Яремча, 2011; the 5-th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2011), - Praga, 2011; міжнародній конференції Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET 2012). – Львів-Славске, 2012.

Публікації. За матеріалами дисертації опубліковано 26 друкованих праць, серед яких 13 статей, з них 7 у фахових наукових виданнях (2 одноосібні), 4 патенти України на корисну модель, 9 робіт опубліковано у збірниках матеріалів конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків та додатків (210 ст.). Основний зміст дисертаційної роботи викладений на 145 сторінках. Дисертація містить 65 рисунків, 29 таблиць та 154 посилання на джерела.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У ***вступі*** наведено загальну характеристику дисертаційної роботи, обґрунтовано її актуальність, сформульовано мету і задачі досліджень, показано наукову новизну і практичну цінність отриманих результатів, виконано постановку задачі досліджень.

У ***першому розділі*** проведений аналіз та виконана систематизація процесорів цифрового опрацювання даних на основі різних архітектур та сфери застосувань в широкому класі задач цифрового опрацювання даних при використанні різних теоретико-числових базисів, що дозволило обґрунтувати перспективу розробки та реалізації високопродуктивних спецпроцесорів опрацювання великорозрядних чисел у системі числення залишкових класів базису Крестенсона. Проаналізовані характеристики структур та побудовані

графи мікропрограм функціонування арифметичних модулів в базисах Радемахера, Крестенсона та Галуа. Побудовані діаграми часової складності виконання арифметико-логічних операцій процесорів різних ТЧБ, що дозволило обґрунтувати перспективу застосування процесорів базису Крестенсона при виконанні операцій додавання та множення. Проаналізовано характеристики арифметико-логічних операцій у базисах Радемахера та Крестенсона, здійснено порівняння функціональних можливостей процесорів та побудовані діаграми часових затрат виконання базових операцій, що дозволило встановити основні переваги процесорів базису Крестенсона при вирішенні задач шифрування інформаційних потоків у сучасних комп'ютерних системах та сформулювати завдання і постановку задачі дисертаційного дослідження.

У ***другому розділі*** дисертаційної роботи викладено теоретичні засади прямого та зворотнього перетворення цілочисельної системи залишкових класів базису Крестенсона. Подано приклад розрахунку базисних чисел B_i та нормуючих коефіцієнтів m_i для взаємопростих модулів p_1, p_2,…, p_i,…p_k. Формалізовано аналітика арифметичних операцій додавання, віднімання, множення в СЗК та розраховані порівняльні характеристики швидкодії виконання арифметико-логічних операцій у базисах Радемахера та Крестенсона. В результаті чого встановлено, що операції сумування та множення в базисі Крестенсона можуть виконуватись за один такт роботи процесора, а при зростанні розрядності опрацьовуваних чисел більше 128 біт швидкодія процесорів базису Крестенсона перевищує відповідні характеристики процесорів базису Радемахера на 2-3 порядки.

Досліджено пряме та зворотне перетворення нормалізованої форми СЗК (НСЗК) та визначені умови необхідної розрядності представлення двійкових кодів нормалізованих залишків $[b_i]_0$ двійковими кодами з фіксованою комою. Розраховано приклад кодування чисел в НСЗК та формалізовано алгоритм виконання операції додавання в НСЗК. Показано, що перевагою НСЗК є виключення операції *mod*P з великою часовою та апаратною складністю по базовому модулю СЗК і заміна її операцією по *mod*1, яка виконується шляхом відкидання цілої частини нормалізованих залишків.

Обґрунтована перспектива розмежування великорозрядних чисел з метою зменшення апаратної та часової складності процесорів міжбазисних перетворень та опрацювання великорозрядних чисел. Теоретичною основою розмежованої СЗК (РСЗК) є цілочисельна форма СЗК, рівняння якої представлено у вигляді суми:

$$N_k = N_{1k} + N_{2k} + ... + N_{ik} + ... + N_{nk},$$

де N_{ik} – m- розрядний (розмежований) фрагмент числа N_k, яке представлене у двійковій системі числення. Наприклад, 1024-х розрядний процесор СЗК може бути розмежований на 32 фрагменти по 32 біти (рисунок 1).

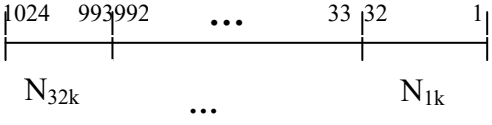
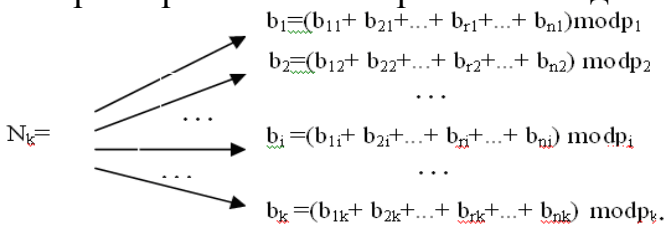


Рисунок 1 – Приклад розмежування 1024-х розрядного процесора.

Таким чином, пряме перетворення РСЗК отримає вигляд:



При цьому математичні операції над числами в РСЗК можуть бути розмежовані по кожному із фрагментів процесора, що забезпечує ще більш глибокий рівень розпаралелення обробки інформації, а, відповідно, підвищення швидкодії процесора СЗК.

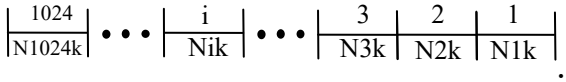
Зі структури розмежованого процесора зрозуміло, що вона потребує обчислення залишків для кожного компонента згідно виразу:

$$b_{ij} = resN_{ij} (\mathrm{mod}\ p_i),$$

де res - символ операції отримання залишку.

Звідки, загальний залишок $b_i = res(b_{i1} + b_{i2} + \ldots + b_{in}) \bmod p_i$.

При бінарному розмежуванні двійкових чисел базису Радемахера, тобто k=0, структура розмежування має наступний вигляд:



Запропонований принцип перетворення чисел базису Радемахера в СЗК на основі теорії РСЗК дозволяє поглибити процес розпаралелювання та спрощення арифметичних операцій базису Крестенсона. В той же час виконання процедури розмежування на N розрядів $N = 2^i \cdot n$, де N – число розрядів процесора, 2^i – коефіцієнт розмежування, приводить до спрощення складних дешифраторів, а також передбачає наскрізні переноси в РСЗК.

Реалізація побітного розмежування чисел в базисі Радемахера дозволяє суттєво спростити алгоритм переходу з базису Радемахера в базис Крестенсона, а також реалізувати повнофункціональну арифметичну операцію у РСЗК без наскрізних переносів та з максимальним розпаралеленням.

У ***третьому розділі*** дисертаційної роботи отримані аналітичні вирази та досліджена часова складність алгоритмів міжбазисних перетворень Радемахера-Крестенсона та Крестенсона-Радемахера на основі цілочисельної, нормалізованої, досконалої та розмежованої форм СЗК, а також міжбазисних перетворень Радемахера-Галуа, Крестенсона-Галуа, Галуа-Радемахера і Крестенсона-Галуа.

В результаті проведених досліджень встановлено, що перетворення Радемахера-Крестенсона та Крестенсона-Радемахера характеризуються найменшою часовою складністю та найбільшим числом міжбазисних перетворень у цілочисельній, нормалізованій, досконалій та розмежованій формах СЗК. Тому такі міжбазисні перетворення можуть бути ефективно застосовані при створенні мультибазисних процесорів, а також опрацюванні великорозрядних чисел в системах криптозахисту інформації та ряді фундаментальних задач теорії чисел.

Вимоги створення швидкодіючих спецпроцесорів опрацювання великорозрядних чисел у базисі Крестенсона визначають доцільність застосування однотактних матричних суматорів по модулю в кодах базису Хаара.

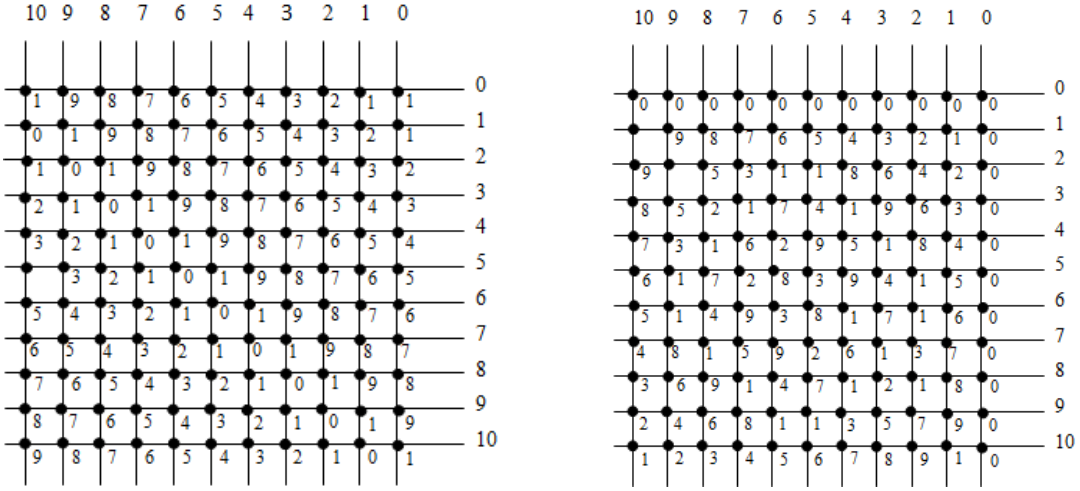
Розроблено метод виконання операцій додавання та множення по модулю у базисі Хаара, який здійснюються згідно аналітичних виразів:

$S_k(H) = res(b_i + b_j) \bmod P$, $Z_k(H) = res(b_i \cdot b_j) \bmod P$;

$S_k = k(H)$, якщо $(b_i + b_j) = P_j + k$, що відповідає $b_i(H) \wedge b_j(H) = 1$;

$Z_k = k(H)$, якщо $(b_i \cdot b_j) = P_j + k$, що відповідає $b_i(H) \wedge b_j(H) = 1$.

На пересіченні шин матриць (рисунок 2) розміщається один логічний елемент «І-НЕ», а вихідний біт формується на основі провідного логічного елемента «АБО», то апаратна складність таких пристроїв рівна $P^2 + P$ та P^2 (рисунок 3), а часова складність рівна $2v$, де v – час переключення мікроелектронного вентиля (нс).



а) б)

Рисунок 2 – Матрично-модульний суматор (а) та перемножувач (б) базису Хаара по модулю 11.

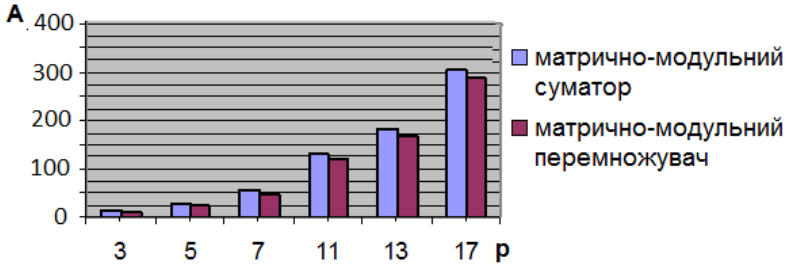


Рисунок 3 – Апаратна складність матрично-модульного суматора та перемножувача у базисі Хаара: А – апаратна складність, р – значення модулів.

Швидке зростання апаратної складності даного класу матрично-модульних пристроїв не дозволяє використовувати їх автономно при опрацюванні великорозрядних чисел. В той же час використання таких пристроїв у процесорах базису Крестенсона є достатньо ефективним, оскільки при переході до базису Крестенсона кількість вентильних елементів замість N^2 буде рівною сумі P_j^2, де P_j – взаємопрості модулі, добуток яких перевищує число N (див. рисунок 3).

Модульна матриця множення у базисі Хаара-Крестенсона реалізується згідно аналогічної структури з часовою складністю $\tau = \nu$ та меншою апаратною складністю без елементів обчислення рангів $A = p^2$.

Проведені дослідження стали основою розробки спецпроцесорів у базисі Хаара-Крестенсона.

Розроблені теоретичні засади та алгоритми виконання міжбазисних перетворень на основі матричних суматорів у розмежованій СЗК пірамідального та лінійного типу. Оцінені характеристики часової та апаратної складності в залежності від розрядності чисел базису Радемахера. В результаті встановлено, що в бінарно-розмежованій СЗК підвищується ефективність реалізації міжбазисного перетворення Радемахера-Крестенсона за схемотехнічними варіантами на основі пірамідально та лінійно з'єднаних суматорів по модулю Р.

Для переходу з базису Радемахера в базис Крестенсона над елементами стрічок матриці, представленої в бінарно-розмежованій системі, виконується наступна операція над залишками:

$$N_k = res(b_{n-1,j} + b_{n-2,j} + ... + b_{i,j} + ... + b_{1,j} + b_{0,j}) \bmod P_i .$$

Для підвищення швидкості модульної операції доцільно застосувати структуру пірамідального алгоритму сумування (рисунок 4). Швидкодія такого пірамідально-модульного суматора $m = i \log_2 n$, де n – розрядність процесора базису Радемахера, i – кількість залишків.

Висока швидкодія такого компонента міжбазисного перетворення Радемахера-Крестенсона потребує великої кількості суматорів в залежності від розрядності процесора, число яких

$$S = n + n/2 + n/4 + ... + n/n .$$

Таким чином, загальний об'єм даного міжбазисного перетворення можна оцінити згідно виразу $Q = K \cdot S$, де К – число взаємопростих модулів базису Крестенсона.

Об'єм мікроелектронного обладнання, міжбазисного перетворювача, можна суттєво зменшити на основі запропонованої структури (рисунок 5).

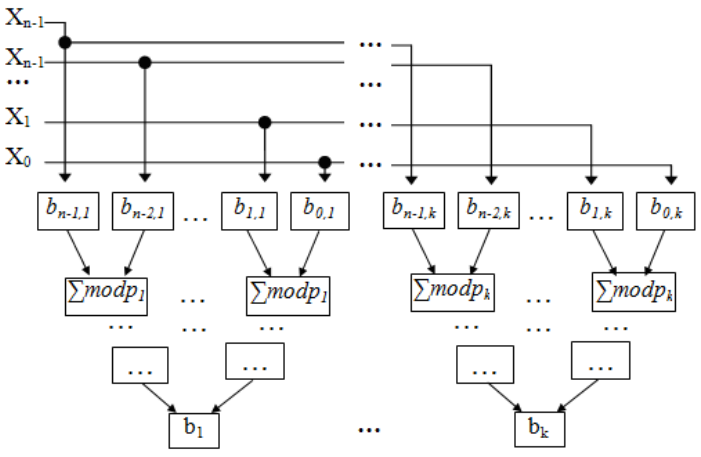


Рисунок 4 – Пірамідальний алгоритм сумування залишків в РСЗК.

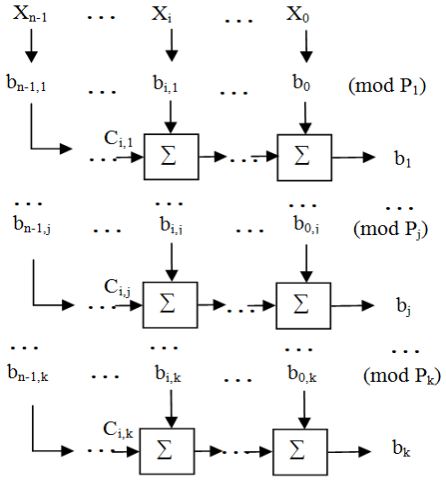


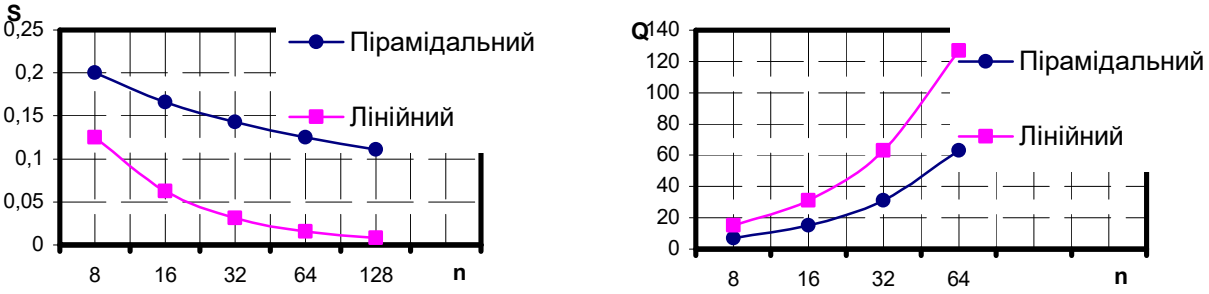
Рисунок 5 – Структура міжбазисного перетворювача Радемахера-Крестенсона.

Отримані характеристики об'єму та швидкодії мікроелектронного обладнання суматора по модулю P_j (рисунок 6).

Результати аналізу швидкодії двох досліджуваних архітектур міжбазисного перетворення (МБП) при унітарному кодуванні залишків (див. рисунок 6) розраховується згідно виразів:

$$S_p = 1/2 + \log_2 n;\ \ S_l = 1/n,$$

де n – число розрядів процесора; S_p – швидкодія пірамідального МБП; S_l – швидкодія лінійного МБП.



а) б)

Рисунок 6 – Швидкодія (а) та об’єм мікроелектронного обладнання (б) міжбазисних перетворювачів Радемахера-Крестенсона.

Проведені дослідження показали, що об’єм обладнання пірамідальної структури в два рази перевищує об’єм лінійної структури при заданій розрядності процесора. Швидкодія пірамідального МБП із збільшенням розрядності процесора від 8 від 128 зростає відповідно від 1,6 до 13,8 разів.

У ***четвертому розділі*** досліджені системні та схемотехнічні характеристики компонентів спецпроцесорів у базисі Крестенсона. Встановлено функціональні переваги апаратної та часової складності модульних матриць сумування, множення та шифрування даних у базисі Крестенсона по відношенню до базису Радемахера, що дозволяє ефективно використати досліджувані компоненти при побудові високопродуктивних спецпроцесорів опрацювання великорозрядних чисел у базисі Крестенсона. Розроблені та досліджені алгоритми піднесення до високих показників степенів у РСЗК.

Розроблено схемотехнічні рішення модульних компонентів спецпроцесорів для великорозрядних чисел у базисі Крестенсона та досліджені їх системні характеристики.

Для реалізації модульних шифраторів Радемахера-Крестенмона при 4-бітній розрядності компонентів процесора оптимальний набір модулів з максимальним діапазоном кодування задається масивом чисел: p_i*=(3, 5, 7, 8, 11, 13),* що відповідає діапазону кодування: *P=120120,* що достатньо для реалізації швидкодіючого 16-бітного процесора в РСЗК.

Часова складність шифраторів Радемахера-Крестенсона на основі структурної схеми з використанням послідовно включених елементів «АБО» пропорційна розрядності модуля p_i у базисі Хаара, тобто $T_{SH} = (p_i + 1)\nu$. При реалізації шифратора на основі схеми «провідне АБО» (рисунок 7) часова складність шифратора суттєво зменшується $T_{SH} = 2\nu$. Відповідно апаратна складність розглянутих схемотехнічних реалізацій шифраторів визначається згідно виразів $A_{SH} = 2^k \cdot (p_i + 1)$ та $A_{SH} = 2^k$, де *k*–розрядність модуля (рисунок 8).

Рисунок 7 – Часова складність шифраторів Радемахера-Крестенсонаю.

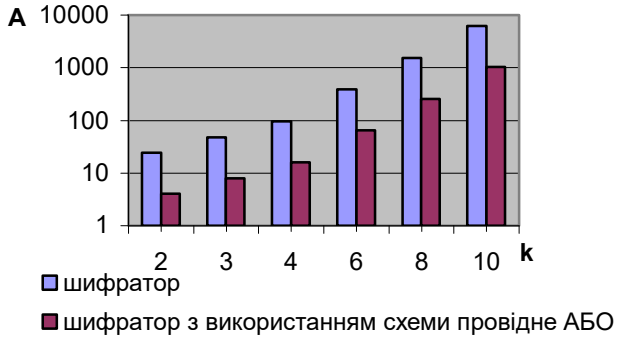


Рисунок 8 – Апаратна складність розглянутих схемотехнічних реалізацій шифраторів Радемахера-Крестенсона.

З наведених діаграм часової та апаратної складностей (див. рисунки 7, 8) видно, що при реалізації шифраторів доцільніше використовувати схеми «провідне АБО», яке дозволяє зменшити апаратну складність в 6 разів.

Вперше розроблено метод отримання залишку з великорозрядного двійкового числа використанням модуля пам'яті. Метод отримання залишку b_i двійкового числа, представленого починаючи з старшого розряду $X = (a_0, a_1, ...a_i ...a_{n-1})$, де $a_i \in \overline{0,1}$ по заданому модулю P_j, описується рекурентною формулою:

$$b_i = (a_i + 2 \cdot b_{i-1}) \bmod P_j, \qquad (1)$$

де a_i –значення i-того біта двійкового числа; b_{i-1}–значення залишку $(i-1)$-го біта двійкового числа. Початкова умова рекурентної формули отримання залишку задається наступними даними: $i = n-1$, $b_{i-1} = 0$. Отримане b_0 – шуканий залишок згідно виразу:

$$b_0 = resX(\bmod P_j).$$

Пристрій обчислення залишку двійкового числа (рисунок 9) працює наступним чином: у регістр пам'яті та зсуву з вхідної шини записується n-розрядний код числа X, молодші розряди якого записуються у відповідні розряди регістра починаючи зліва, а в інші m розряди записуються нулі. Одночасно з вхідної шини в постійний запам'ятовуючий пристрій подається m-розрядний двійковий код модуля P. Після n зсувів з вихідної шини зчитують код кінцевого залишку b_0 числа X по модулю P, починаючи зі старшого розряду справа.

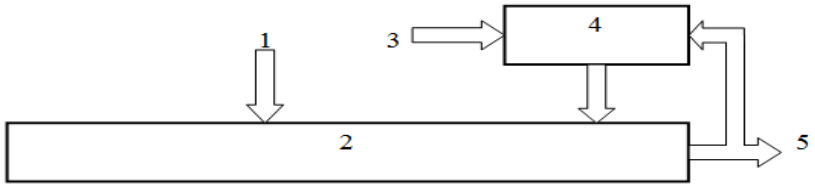


Рисунок 9 – Структура пристрою визначення залишку двійкового числа з використанням ПЗП: 1 – вхідна шина двійкового числа X та залишку $b_0=0$; 2 – $(n+m)$-розрядний регістр пам'яті та зсуву; 3 – вхідна шина m-розрядного коду модуля P; 4 – постійний запам'ятовуючий пристрій; 5 – вихідна шина проміжного та кінцевого залишку b_0 по модулю P.

Слід зазначити, що часова складність відомого алгоритму буде обчислюватись згідно наступного співвідношення: $O2(n) = mn^2 + mn + m^2 n + 2n - 2m + 1$. Скориставшись пірамідальним алгоритмом для обчислення залишку отримаємо наступний вираз часової складності: $O3(n) = n\log^2(n)$.

Часова складність розробленого методу обчислення залишку великорозрядних чисел по заданому модулю згідно рекурентного співвідношення (1): обчислюються згідно виразу: $O1(n) = 2n$.

Результатом чисельного експерименту показано (рисунок 10), що розроблений метод характеризується меншою часовою складністю на 2-3 порядки в порівнянні з відомими.

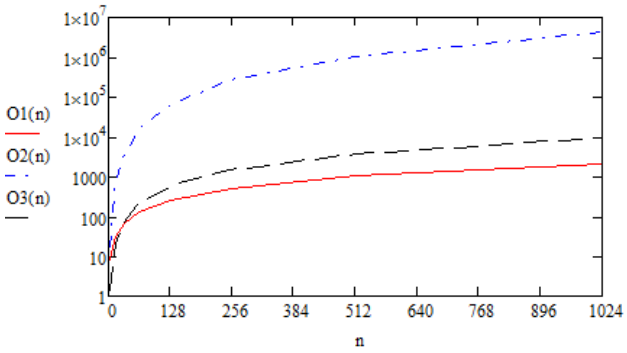


Рисунок 10 – Часова складність обчислення залишків по модулю.

Отже, враховуючи проведені дослідження розроблений метод на основі використання рекурентного співвідношення доцільно використовувати в міжбазисних перетвореннях.

Реалізовано міжбазисний перетворювач Радемахера-Крестенсона на основі структури визначення залишку двійкового числа з використанням ПЗП (див.рисунок 9) шляхом вбудови в кожний канал такого перетворювача по модулю P.

Апаратна складність такого міжбазисного перетворювача обчислюється згідно формули $A = n \cdot 2ЛЕ + \mathrm{k} \cdot 2ЛЕ + A_{ПЗП}$, де n – розрядність процесора, $ЛЕ$ – логічний елемент, k - розрядність модуля, $A_{ПЗП}$ - апаратна складність ПЗП. Апаратна складність ПЗП визначається наступним чином: $A_{ПЗП} = 2\mathrm{p} \cdot \mathrm{k}$, де $\mathrm{k} = \hat{E}[\log_2 p]$ (рисунок 11).

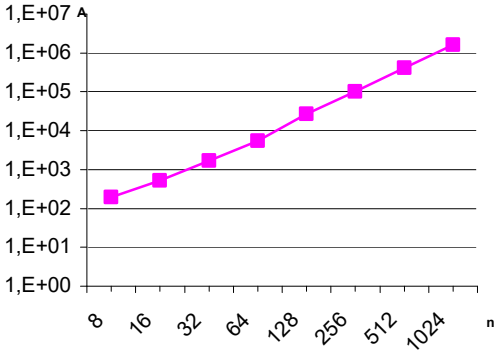


Рисунок 11 – Апаратна складність міжбазисного перетворювача з використанням ПЗП.

Вперше розроблений та реалізований метод міжбазисного перетворення Радемахера-Крестенсона на основі комутованих рандомізаторів шляхом глибокого розпаралелення процесів опрацювання бітів великорозрядних чисел базису Радемахера, що дозволило досягнути максимальної швидкодії перетворення та отримати всі коди залишків n, k розрядного перетворення Радемахера-Крестенсона.

Міжбазисний перетворювач Радемахера-Крестенсона ілюструється структурною схемою (рисунок 12), де 1 – вхідні шини k –розрядного позиційного

числа, 2 – комутаційні мультиплексори, 3 – виходи коду b_i системи залишкових класів.

На рисунку 13 зображена структурна схема комутаційного мультиплексора по модулю 7 (2.1– рандомізатор по модулю p_j, 2.2 – інкрементний пристрій по модулю p_i, 2.3 – p-канальний двохвходовий мультиплексор).

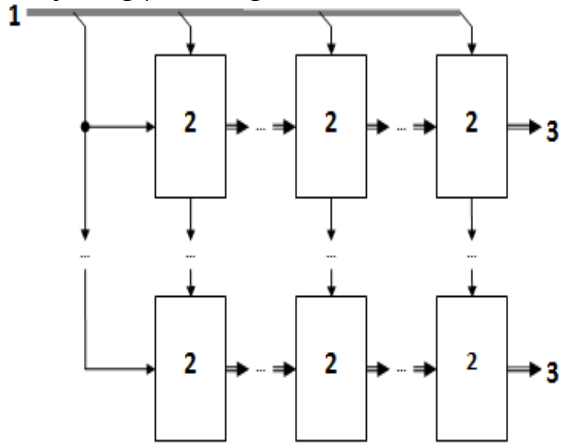


Рисунок 12 – Структурна схема перетворювача Радемахера-Крестенсона на основі рандомізаторів.

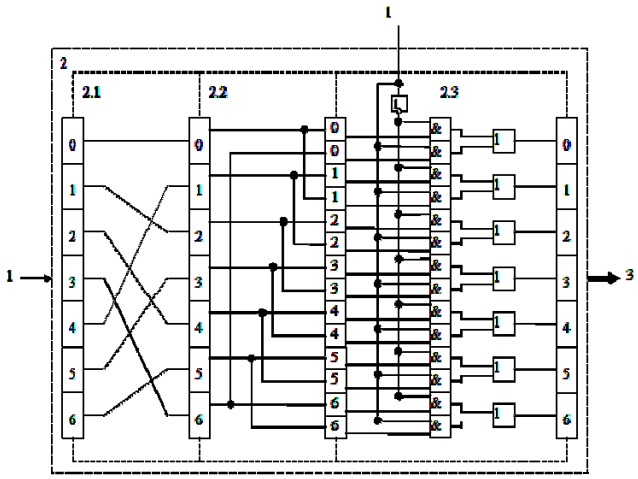


Рисунок 13– Структура комутаційного мультиплексора.

Оцінку часової складності спецпроцесора міжбазисного перетворення на основі рандомізаторів та мультиплексорів розраховуємо згідно виразу: $\tau = 2\nu$, що відповідає тривалості переключення двох послідовно підключених вентильних елементів мультиплексора. Оскільки всі мультиплексори переключаються одночасно при подаванні на їх входи бітових значень великорозрядного двійкового числа, то швидкодія такого міжбазисного перетворювача не залежить від розрядності перетворюваного числа базису Радемахера.

Оцінка апаратної складності розробленого міжбазисного перетворювача розраховується згідно виразу $A = 3p + 1 + (9p \cdot 0.001)$, де 0,001 – апаратна складність комутаційних з'єднань рандомізатора (рисунок 14).

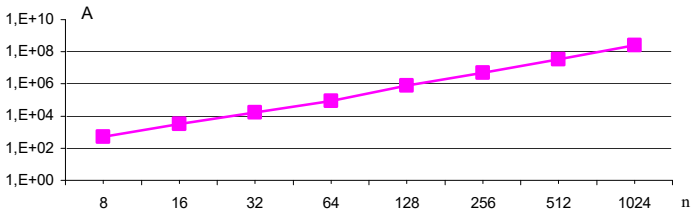


Рисунок 14 – Апаратна складність міжбазисного перетворювача на основі рандомізаторів.

Розроблено метод обчислення залишку багаторозрядного двійкового числа Y по багаторозрядному цілочисельному модулю P згідно рекурсивного виразу:

$$b_i = [p]_{мд} + 2b_{i-1} + a_i, \quad i = n, n-1, ..., 1,$$

де n – розрядність числа Y, з якого визначається залишок b_i, a_i – біти двійкового числа Y, починаючи зі старшого розряду a_n, $[p]_{мд}$ – $k+1$ розрядна мантиса доповнюючого коду модуля P, b_i – поточне кодове значення залишку ($b_{i-1} = 0$).

Розроблена функціональна схема визначення залишку багаторозрядного числа (рисунок 15) та розраховані її системні характеристики.

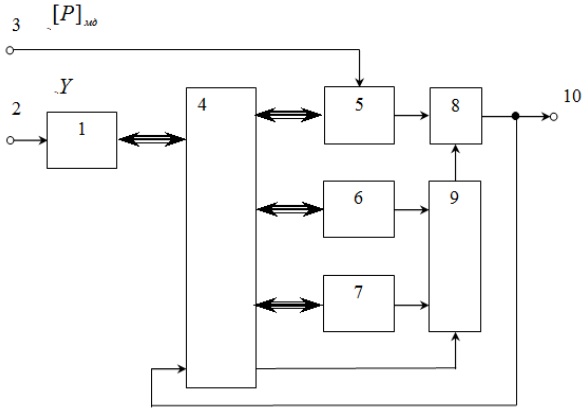


Рисунок 15 – Функціональна схема спецпроцесора обчислення залишку великорозрядних чисел: 1 – перший n-розрядний регістр зсуву, 2 – шина запису кодового представлення числа Y, 3 – шина запису кодового представлення модуля P, 4 – блок управління, 5 – другий k+1-розрядний регістр зсуву, 6 – третій k+1-розрядний регістр зсуву, 7 – четвертий k+1-розрядний регістр зсуву, 8 – однорозрядний накопичувальний суматор, 9 – мультиплексор, 10 – вихідна шина кодового представлення залишку b_i.

На початку циклів визначення залишку числа Y у перший n-розрядний регістр зсуву і другий k+1-розрядний регістр зсуву, згідно адресних сигналів блоку управління відповідно записуються двійковий код числа Y та мантиса доповнюючого коду модуля P, а в третій і четвертій k+1-розрядні регістри зсуву записуються нулі. На початку кожного наступного циклу роботи пристрою на четвертому виході блоку управління формується сигнал «1», що дозволяє зсув на один розряд в бік старших розрядів коду залишку b_{i-1} у регістрі та запис старшого біта числа Y a_i у молодший розряд третього регістра, що відповідає запису в цей регістр $2b_{i-1} + a_i$.

В кожному поточному циклі роботи пристрою одночасно через мультиплексор на входи однорозрядного накопичувального суматора, порозрядно зчитується код мантиси модуля $P([P]_{мд})$ розрядністю $k+1$ та код відповідного регістра. При цьому одночасно відбувається запис нового залишку b_i у відповідний регістр згідно адресних входів блоку управління.

Графіки швидкодії розглянутих пристроїв представлені на рисунку 16, аналітичні вирази яких мають наступний вигляд:

$$S = 1/(2(n-1)),$$

де $S(n)$ - кількість залишків з розрядністю n, що процесор обчислює в унітарному коді за 1с;

$$S1 = p/2^n,$$

де $S1(n)$ - кількість залишків з розрядністю n, що процесор обчислює в двійковому коді базису Радемахера за 1с, p - модуль;

$$S2 = 4^{20-n},$$

де $S2(n)$ – кількість залишків з розрядністю n, що процесор обчислює в базисі Крестенсона за 1с.

На рисунку 17 подано результати дослідження при використанні елементної бази різних виробників.

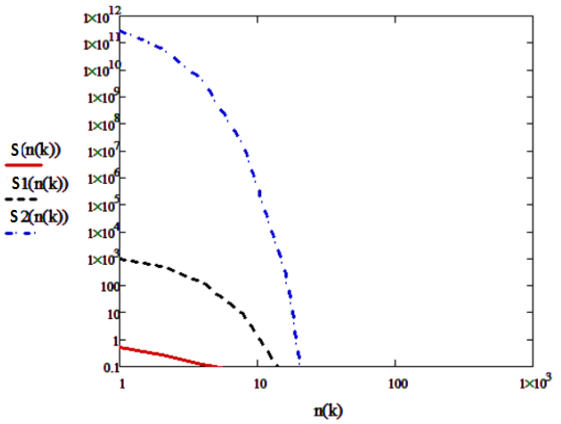


Рисунок 16 – Швидкодія пристроїв обчислення залишків по модулю.

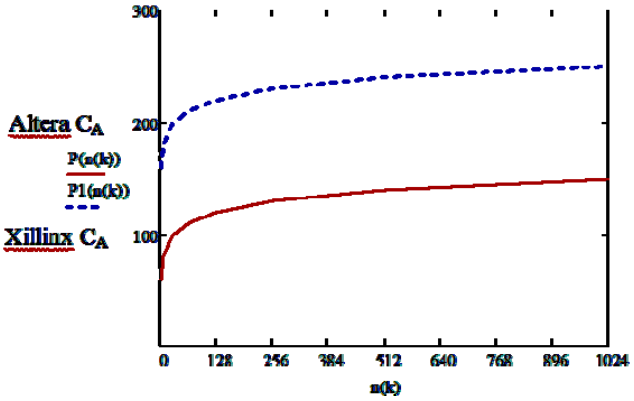


Рисунок 17 – Апаратна складність запропонованого методу при використанні елементної бази різних виробників.

Результати чисельного експерименту показали, що використання елементної бази фірми Xilinx при проектуванні спецпроцесора обчислення залишків по заданому модулю дозволяє зменшити апаратну складність на 20% порівняно з елементною базою фірми Altera. Платформа оснащена модулем інтерфейсу PCI, що дозволяє імплементовувати її в існуючі обчислювальні системи як окремий елемент. Особливістю даної платформи є сумісне використання ПЛІС XilinxSpartanIII та AlteraCyclone, які мають доступ до спільної оперативної пам'яті SRAM розміром 16Мб, що дозволяє провести дослідження та аналіз системних характеристик спецпроцесора на різних кристалах.

ВИСНОВКИ

У дисертаційній роботі розв'язана актуальна наукова задача розробки та реалізації методів побудови високопродуктивних спецпроцесорів на основі використання теоретико-числового базису Крестенсона.

При цьому отримані наступні результати:

1. Виконана систематизація процесорів цифрового опрацювання даних на основі різних архітектур та використання різних теоретико-числових базисів, що дозволило обґрунтувати перспективу розробки та реалізації високопродуктивних спецпроцесорів опрацювання великорозрядних чисел у системі числення залишкових класів базису Крестенсона.

2. Виконаний аналіз характеристик арифметико-логічних операцій у базисах Радемахера та Крестенсона, здійснено порівняння функціональних можливостей процесорів та побудовані діаграми часових затрат виконання базових операцій, що дозволило встановити основні переваги процесорів Крестенсона при вирішенні задач шифрування інформаційних потоків у сучасних комп'ютерних системах та сформулювати завдання і постановку задачі дисертаційного дослідження.

3. Викладені теоретичні засади прямого та зворотнього перетворення цілочисельної системи залишкових класів базису Крестенсона. Поданий приклад розрахунку базисних чисел B_i та виконання арифметико-логічних операцій у базисах Радемахера та Крестенсона, в результаті чого встановлено, що операції сумування та множення в базисі Крестенсона можуть виконуватись за один такт роботи процесора, а при зростанні розрядності опрацьовуваних чисел більше 128 біт швидкодія процесорів базису Крестенсона перевищує відповідні характеристики процесорів базису Радемахера на 2-3 порядки.

4. Розроблено алгоритм операції ділення на основі бінарно-розмежованої СЗК та отримано аналітичну матрицю цієї операції у базисі Крестенсона, що дозволило замінити операцію ділення операцією множення в розширеній СЗК та

доповнюючими кодами залишків і виконувати її за обмежене число тактів процесора з підвищенням швидкодії виконання операції ділення на 2-3 порядки.

5. Розроблені принципи та теоретичні основи розмежування розрядної сітки у базисі Радемахера-Крестенсона, у результаті чого отримані аналітичні вирази прямого та зворотнього перетворень розмежованої системи. Показано, що при бінарному розмежуванні базису Радемахера формуються матриці степеневих залишків двійкових чисел, які дозволяють зменшити на 2-3 порядки алгоритмічну та часову складність міжбазисних перетворень, а також операцій додавання, множення та піднесення до степеня великорозрядних двійкових чисел.

6. Отримані аналітичні вирази та досліджена часова складність алгоритмів міжбазисних перетворень Радемахера-Крестенсона та Крестенсона-Радемахера. Розрахована та побудована діаграма алгоритмічної складності досліджених міжбазисних преретворень.

7. Розроблені теоретичні засади та алгоритми виконання міжбазисних перетворень на основі матричних суматорів у розмежованій СЗК пірамідального та лінійного типу, в результаті встановлено, що в бінарно-розмежованій СЗК підвищується ефективність реалізації міжбазисного перетворення Радемахера – Крестенсона за схемотехнічними варіантами на основі пірамідально та лінійно з'єднаних суматорів по модулю P, при чому, об'єм обладнання пірамідальної структури в два рази перевищує об'єм лінійної структури при заданій розрядності процесора. Швидкодія пірамідального МБП із збільшенням розрядності процесора від 8 до 128 зростає відповідно від 1,6 до 13,8 разів.

8. Запропоновані рекурентні алгоритми та високопродуктивні спецпроцесори опрацювання великорозрядних чисел у базисі Радемахера-Крестенсона шляхом використання однорозрядного двійкового суматора та ПЗП в якості обчислювача поточних сум залишків по модулю, що дозволило зменшити на порядок апаратну складність та підвищити на 2 порядки швидкодію спецпроцесорів даного класу.

9. Розроблені та досліджені системні та схемотехнічні характеристики компонентів спецпроцесорів у базисі Крестенсона. Встановлено функціональні переваги апаратної та часової складності модульних матриць сумування, множення та шифрування даних у базисі Крестенсона по відношенню до базису Радемахера.

10. Розроблено високопродуктивний спецпроцесор міжбазисного перетворення Радемахера-Крестенсона, що, у порівнянні з відомими аналогами, шляхом мультиплексування та рандомізації розмежованих залишків дозволило досягнути максимальної швидкодії визначення кодів залишків, у системі взаємопростих модулів, з часовою складністю перемикання двох послідовно з'єднаних логічних вентилів, незалежно від розрядності перетворюваного двійкового числа.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Волинський О.І. Методи міжбазисних перетворень на основі розмежованої системи числення залишкових класів / О.І. Волинський // Вісник національного університету "Львівська політехніка", "Комп'ютерні системи та мережі". – 2010. - №688. - С.53-59.

2.Волинський О.І. Методи високопродуктивних перетворень великорозрядних чисел з базису Радемахера у базис Крестенсона / О.І. Волинський // Вісник національного університету "Львівська політехніка", "Комп'ютерні системи та мережі". – 2012. - №745. – С.39-48.

3. Николайчук Я.М. Теоретичні основи побудови та структура спецпроцесорів в базисі Крестенсона / Я.М. Николайчук, О.І Волинський, С.В.Кулина // Вісник Хмельницького національного університету. – 2007. - №3. – Т1. – С. 85-90.

4. Николайчук Я.М. Швидкодіючий алгоритм та процесор порівняння чисел у системі залишкових класів / Я.М. Николайчук, О.І Волинський, С.В.Кулина // Науково-теоретичний журнал "Искусственный интеллект". ІПШІ МОН і НАН України "Наука і освіта". – 2008. – №3. – С.348-352.

5. Касянчук М.М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера-Крестенсона / М.М. Касянчук, І.З.Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету, Видавництво Хмельницького національного університету. – 2011. – № 3(177). – С.265-272.

6. Волинський О.І. Систематизація характеристик теоретико-числових базисів та їх застосування для побудови високопродуктивних спецпроцесорів/ О.І.Волинський, В.Пуюл // Вісник Тернопільського національного технічного університету “Науковий журнал”. – Тернопіль – 2011 – Том 16.№3. – С.183-189

7. Албанський І.Б. Дослідження системних характеристик цифрових пристроїв множення реалізованих в різних теоретико-числових базисах / І.Б. Албанський, О.І. Волинський // Вісник Хмельницького національного університету. – 2012. – №2. – С. 179-186.

8. Патент на корисну модель № 68872. МПК G 06 F7/00. Опублікований 10.04.2012. Бюл.№7. Николайчук Я.М., Якименко І.З., Воронич А.Р., Волинський О.І. / Пристрій визначення залишку багаторозрядного числа.

9. Патент на корисну модель № 74576. МПК G 06 F5/00. Опублікований 12.11.2012. Бюл.№21. Николайчук Я.М., Волинський О.І. / Спосіб визначення залишку двійкового числа.

10. Патент на корисну модель № 76623 МПК G06F5/02 Опублікований 10.01.2013 Бюл.№1. Николайчук Я.М., Волинський О.І. / Пристрій для перетворення чисел з позиційної системи в систему залишкових класів.

11. Патент на корисну модель № 76622.МПК G 06F 17/15 Опубл. 10.01.2013 Бюл.№1. Николайчук Я.М., Албанський І.Б., Волинський О.І. / Цифровий автокорелятор.

12. Николайчук Я.М. Теорія побудови та компоненти швидкодіючих процесорів на основі досконалої та розмежованої форм системи залишкових класів / Я.М. Николайчук, О.І Волинський, С.В.Кулина // Поступ в науку. Збірник праць Бучацького інституту менеджменту і аудиту. – 2008. – №4. - Т1. – С.31-36.

13. Николайчук Я.М. Теорія та техніка високопродуктивних мультибазисних процесорів / Я.М. Николайчук, О.Д.Круцкевич, С.В.Кулина, О.І.Волинський // Праці міжнародного симпозіуму. Питання оптимізації обчислень. (ПОО - XXXV) . - Київ. – 2009.– Т2. – С.165-169.

14. Волинський О.І. Методи порівняння та сумування в розмежованій системі числення /О.І. Волинський// Поступ в науку. Збірник наукових праць Бучацького інституту менеджменту і аудиту. – 2009. – №5. Т1. – С.91-94.

15. Orest Volinskiy. Methods of interbase transformations are on the basis of the delimited scale of notation of remaining classes / Orest Volinskiy // Proceedings of the 4-th International conference “Advanced Computer Systems and Networks: Design and Application” (ACSN-2009). – Львів. - 2009. – №4. –С.314-317.

16. Волинський О.І. Розмежована система числення залишкових класів та спецпроцесори на її основі / О.І. Волинський, І.З. Якименко // Поступ в науку. Збірник наукових праць Бучацького інституту менеджменту і аудиту . – Бучач. – 2010. – №6. Т1. – С.80-83.

17. Orest Volinskiy. An algorithm of calculation of degrees of numbers is in the delimited system of remaining classes(DSRC) /O.I. Волинський// Proceedings of the X-th International conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2010). – 2010. – №10. –С.305.

18. Orest Volynskyy. Multibases special processor module and correlations processing of information flows / Orest Volynskyy, Ivan Albanskiy, Petro Humenniy, Ostap Krutskevych, Volodymyr Puyul // Proceedings of the XIth International conference"The experience of designing and application of CAD systems in micro-electronics.– 2011. - №11 – С.176-177.

19. Волинський О.І. Методи ділення великорозрядних чисел в теоретико-числовому базисі Радемахера-Крестенсона / О.І.Волинський // Поступ в науку. Збірник наукових праць Бучацького інституту менеджменту і аудиту . – Бучач. – 2011. – №7. Т1. –С.37-39.

20. Івасьєв С.В. Метод знаходження залишків велико-розрядних чисел в базисі Радемахера / С.В. Івасьєв, О.І. Волинський // Поступ в науку. Збірник наукових праць Бучацького інституту менеджменту і аудиту. – 2011.– №7. Т1. –С.88-91.

21. Волинський О.І. Швидкодія міжбазисних перетворювачів Радемахера-Крестенсона / О.І.Волинський // Збірник матеріалів проблемно-наукової міжгалузевої конференції "Юриспруденція та проблеми інформаційного суспільства"(ЮПІС - 2011)" - Івано-Франківськ, 2011. - С.71-75

22. Волинський О.І. Оптимізація обчислень на основі алгоритмів міжбазисних перетворень Радемахера, Крестенсона та Галуа / О.І.Волинський, О.Д. Круцкевич, П.В. Гуменний // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Інститут кібернетики імені В.М. Глушкова НАН України, – Київ 2011. – С. 32-33.

23. Yaroslav Nykolaychuk. Rademacher-Krestenson's method of between-bases transformations in designing processors / Yaroslav Nykolaychuk, Orest Volynskyy, Andrii Borovyi // Proceedings of the 6th International Conference "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications". – Prague, Czech Republic. –2011. – С.310-313.

24. Ivan Albanskiy. Structure and Simulation of Interactive Computer Systems Based on Multibasises Switching Processors / Ivan Albanskiy, Petro Humenniy, Orest Volinskiy, Tanya Zavedyuk // Proceedings of the XI-th International conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2012). – Lviv-Slavsk. – 2012. – С.434.

25. R. Tsanko. Theory, Topology and Building Technology of Multibasis Specialized Processor / R. Tsanko, O. Volynskyy, V. Puyul, I. Pituh // Proceedings of the XI-th International conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2012). – Lviv-Slavsk. – 2012. – С. 260.

26. Волинський О.І. Теорія, алгоритми та спецпроцесори міжбазисних перетворень Радемахера-Крестенсона / О.І.Волинський // Поступ в науку. Збірник наукових праць Бучацького інституту менеджменту і аудиту. – Бучач. - 2012.- №8. С. 50-54.

АНОТАЦІЯ

Волинський О.І. Методи побудови високопродуктивних спецпроцесорів на основі теоретико-числового базису Крестенсона. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти. Тернопільський національний економічний університет, Тернопіль 2013.

У дисертаційній роботі вперше розроблені метод виконання операції модулярного множення у розмежованій матрично-модульній системі числення, який дозволяє зменшити обчислювальну складність модульних операцій множення та експоненціювання на 2-3 порядки у порівнянні з відомими. Вперше розроблено метод перетворення чисел з базису Радемахера в базис Крестенсона рекурентним скануванням двійкових чисел, починаючи зі старшого розряду, що, дозволило виключити операції порівняння та віднімання великорозрядних двійкових чисел з наскрізними переносами і підвищити швидкодію міжбазисного перетворення пропорційно розрядності двійкового числа. Вперше розроблено метод швидкодіючого перетворення чисел з позиційної системи базису Радемахера в систему залишкових класів базису Крестенсона, який шляхом бінарного розмежування, мультиплексування та рандомізації кодів залишків по модулю дозволяє максимально розпаралелити процес визначення кінцевого залишку, швидкодія якого не залежить від розрядності перетворюваних двійкових чисел.

На основі запропонованого методу виконання операції модулярного множення у розмежованій матрично-модульній системі числення розроблений пристрій визначення залишків багаторозрядного числа, який формує коди залишків розмежованої матрично-модульної системи числення у базисі Радемахера-Крестенсона, який шляхом заміни великорозрядного двійкового суматора однорозрядним повним суматором та регістрами зсуву розширює його функціональні можливості при опрацюванні великорозрядних чисел у задачах шифрування інформаційних потоків.

Ключові слова: теоретико-числові базиси Радемахера, Крестенсона, спецпроцесор, міжбазисні перетворення, система залишкових класів, бінарно-розмежована система, модульні компоненти спецпроцесора.

Волынский О.И. Методы построения высокопроизводительных спецпроцессоров на основе теоретико-числового базиса Крестенсона. - Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 - Компьютерные системы и компоненты. Тернопольский национальный экономический университет, Тернополь 2013.

В диссертационной работе впервые разработаны метод выполнения операции модулярного умножения в разграничены матрично-модульной системе счисления, который, по сравнению с известными, отличается тем, что каждый элемент матрицы, соответствующий двоичному разряду второй, представляется кодом остатка по модулю Р, а операция умножения выполняется путем добавления текущих остатков первого числа с их удвоенными значениями по модулю Р, соответствующие единичным элементам кода второго числа, что позволяет уменьшить вычислительную сложность модульных операций умножения и экспоненциирование на 2-3 порядка. Впервые разработан метод преобразования чисел из базиса Радемахера в базис Крестенсона рекуррентным сканированием двоичных чисел, начиная со старшего разряда, что, в отличие от известных преобразований, путем адресной выборки кодов остатков с модуля памяти исключает операции сравнения и вычитания великоразрядных двоичных чисел со

сквозными переносами и позволяет повысить быстродействие междубазисного преобразования пропорционально разрядности двоичного числа. Впервые разработан метод быстродействующего преобразования чисел из позиционной системы базиса Радемахера в систему остаточных классов базиса Крестенсона, который, в отличие от известных, путем бинарного разграничения, мультиплексирования и рандомизации кодов остатков по модулю позволяет максимально распараллелить процесс определения конечного остатка, быстродействие которого зависит от разрядности преобразуемых двоичных чисел.

На основе предложенного метода выполнения операции модулярного умножения в разграниченой матрично-модульной системе счисления разработанное устройство определения остатков многоразрядного числа, который формирует коды остатков разграничены матрично-модульной системы счисления в базисе Радемахера-Крестенсона, который, по сравнению с известными аналогами, путем замены великоразрядного двоичного сумматора одноразрядным полным сумматором и регистрами сдвига, характеризуется повышенным быстродействием и уменьшенной аппаратной сложности, что расширяет его функциональные возможности при обработке великоразрядных чисел в задачах шифрования информационных потоков.

Ключевые слова: теоретико-числовые базисы, базис Радемахера, базис Крестенсона, спецпроцессор, междубазисные преобразования, система остаточных классов, бинарно-разграничена система, модульные компоненты спецпроцессора.

O. Volynskyy. Methods of high-performance special processors constructing that are based on the theoretical and numerical basis of Krestenson. - Manuscript.

PhD thesis (Candidate of technical science) in specialty 05.13.05 –computer systems and components. – Ternopil National Economic University, Ternopil, 2013.

In this scientific work we firstly developed a operation method of modular multiplication, in differentiated matrix-modular number system, which reduces the computational complexity of modular multiplications and exponentiations from 2 to 3 orders in comparison with the known systems. We also firstly developed a method for converting numbers from basis of Rademacher to basis of Krestenson using by recurrent scanning of binary numbers, starting with senior level so this allowed to exclude the operation of comparison and subtraction for large binary numbers with pass-through transfer and to improve the performance of interbasis conversion of proportional category of binary number. There was also firstly developed a method of fast converting numbers from Rademacher positional basis system to Krestenson residual classes basis that by means of binary division multiplication and randomization of residues modulo codes keeps maximally separate the determination process of the final balance, the performance of which does not depend on the converted bit binary numbers category.

Based on the proposed method of modular multiplication operation, in separated modular-matrix number system we developed the device for residues multidigit numbers identification, which forms residue codes of separated matrix-modular number system in Rademacher-Krestenson basis that extends its functional capabilities by means of replacing multy-category binary sumator to single-category sumator and shift register under the process of multy-category number processing in encrypting data flows tasks.

Keywords: theoretical and numerical bases, Rademacher basis, Krestenson basis, special processors, interbasis conversion system of residual classes, binary-differentiated system, special processor modular components.