Розроблення та дослідження високоефективних архітектур спеціалізованих комп'ютерних систем для реалізації обчислень у скінченних полях

Разработка и исследование высокоэффективных архитектур специализированных компьютерных систем для реализации вычислений в конечных полях

Development and Research of Highly Efficient Architectures of Special Purpose Computer System for Implementing Computing in Finite Fields

1. **Номер державної реєстрації теми - 0115U000319,**
2. **Науковий керівник -** д.т.н., професор Дичка І.А., Дичка И.А., Dychka Ivan A.
3. **Суть розробки, основні результати.**

(укр.)

Розроблено модифікований віконний метод піднесення до степеня елементів поля $GF(p)$, чотири алгоритми реалізації цього методу та відповідне програмне забезпечення. Ідею запропонованого методу можна застосовувати для задачі скалярного множення точки еліптичної кривої над довільним скінченним полем.

Розроблене програмне забезпечення показало, що запропонований метод дає приріст швидкодії порівняно з існуючими до 15%, як для піднесення до степеня в скінченному полі, так і для скалярного множення на еліптичній кривій, що задана над скінченним полем. Розроблено методи, алгоритми і програмне забезпечення для виконання операцій за модулем $2^m - 1$. Розроблено табличний метод виконання операцій над елементами поля $GF(2^m)$. Розроблений метод доцільно застосувати для $m \leq 20$. Розроблено програмні та апаратні засоби для реалізації табличного методу виконання операцій над елементами поля $GF(2^m)$. Розроблено спосіб розрідженого зберігання таблиці елементів поля $GF(2^m)$, який дозволяє скоротити об'єм необхідної оперативної пам'яті для зберігання елементів поля $GF(2^m)$.

Результатом проекту є створення архітектури спеціалізованого процесора, що орієнтований на виконання обчислень у полях Галуа, приріст швидкодії порівняно з універсальною обчислювальною системою у 2.4 – 3 рази рази. Розроблено систему команд процесора Галуа та програмну реалізацію компілятора.

(рос.)

Разработан модифицированный оконный метод возведения в степень элементов поля $GF(p)$, четыре алгоритмы реализации этого метода и соответствующее программное обеспечение. Идею предложенного метода можно применять для задачи скалярного умножения точки эллиптической кривой над произвольным конечным полем.

Разработанное программное обеспечение показало, что предложенный метод дает прирост быстродействия по сравнению с существующими до 15%, как для возведения в степень в конечном поле, так и для скалярного умножения на эллиптической кривой, заданной над конечным полем. Разработаны методы, алгоритмы и программное обеспечение для выполнения операций по модулю $2^m - 1$. Разработан табличный метод выполнения операций над элементами поля $GF(2^m)$. Разработанный метод целесообразно применять для $m \leq 20$. Разработаны программные и аппаратные средства для реализации табличного метода выполнения операций над элементами поля $GF(2^m)$. Разработан способ разреженного хранения таблицы элементов поля $GF(2^m)$, который позволяет сократить объем необходимой оперативной памяти для хранения элементов поля $GF(2^m)$.

Результатом проекта является создание архитектуры специализированного процессора, ориентированного на выполнение вычислений в полях Галуа, прирост быстродействия по сравнению с универсальной вычислительной системой в 2.4 – 3 раза. Разработана система команд процессора Галуа и программная реализацию компилятора.

(англ.)

The modified method window exponentiation elements of field $GF(p)$, four algorithms implementing this method and software was proposed. The idea of the proposed method can be applied to the problem of scalar multiplication of points of an elliptic curve over an arbitrary finite field.

The developed software has shown that the proposed method gives performance gains compared to the existing 15%, both for exponentiation in a finite field, and scalar multiplication on elliptic curve defined over a finite field. The proposed methods, algorithms and software to perform modulo $2^m - 1$. Developed tabular method of operations over the elements of the field $GF(2^m)$. The method should be used for $m \leq 20$. The software and hardware to implement tabular method of operations over the elements of the field $GF(2^m)$ was created. A method of storing sparse table of elements of the field $GF(2^m)$, which reduces the amount of memory required to store the elements of the field $GF(2^m)$.

The project is the creation of a specialized processor architecture that is aimed at performing calculations in Galois fields, the increase in speed compared to the universal computer system 2.4 – 3 times. The processor command system and software implementation Galois compiler was develop.

4. Наявність охоронних документів на об'єкти права інтелектуальної власності.

- Схема для пошуку мультиплікативно оберненого елемента за довільним модулем [Текст]: Державний патент України на корисну модель МПК G06F 7/50 / Дичка І.А., Онай М.В., Приходько Е.В. / заявник: Дичка Іван Андрійович (UA), Онай Микола Володимирович (UA), Приходько Ернест Вікторович (UA) — №u201604179; дата подачі заявки: 15.04.2016; дата публ. 10.11.2016, бюл. №21, 2016 р.
- Система автоматизованого моніторингу транспортного потоку [Текст]: Державний патент України на винахід МПК G08G 1/050 (2006.01), G08G 1/017 (2006.01), G07C 5/08 (2006.01) / Бухтіяров Ю.В., Балабанова О.І. / заявник: Бухтіяров Юрій Вікторович (UA) — №a201405406; дата подачі заявки: 21.05.2016; дата публ. 11.04.2016, бюл. №7, 2016 р.

5. Порівняння зі світовими аналогами.

Результати відповідають світовому рівню, а розроблена архітектура спеціалізованого процесора, що орієнтований на виконання обчислень у полях Галуа, не має аналогів у світовій практиці.

6. Економічна привабливість для просування на ринок

Застосування розробленої архітектури спеціалізованого процесора, що орієнтований на виконання обчислень у полях Галуа, дозволяє значно знизити собівартість спеціалізованих обчислювальних засобів та прискорити час роботи алгоритмів завадостійкого кодування та криптографічного захисту інформації за рахунок використання нового способу побудови таблиць передобчислень в алгоритмах піднесення до степеня.

7. Потенційні користувачі (галузі, міністерства, підприємства, організації).

Результати роботи можуть бути використані підприємствами-розробниками систем обробки сигналів, автоматичної ідентифікації об'єктів, промислових систем контролю за переміщенням об'єктів.

Підтвердили зацікавленість в результатах роботи такі організації:

- Українське державне підприємство поштового зв'язку (УДППЗ) «Укрпошта» (Міністерство транспорту та інфраструктури України).
- ТОВ «Відео Інтернет Технології».

На базі цих підприємств буде підготовлена документація для впровадження результатів роботи у виробництво.

На УДППЗ «Укрпошта» результати роботи будуть використані при впровадженні технології цифрових поштових марок, а в ТОВ «Відео Інтернет Технології» – в системах обробки та аналізу зображень для розпізнавання реєстраційних номерів транспортних засобів.

8. Стан готовності розробки.

Розроблено модель процесора Галуа на мові Verilog, розроблено систему команд Асемблера процесора Галуа, розроблено інтегроване середовище для написання тексту програми на мові Асемблера процесора Галуа та трансляції у машинний код.

9. Існуючі результати впровадження.

Розроблений віконний метод піднесення до степеня елементів поля $GF(p)$ та табличний метод виконання операцій над елементами поля $GF(2^m)$ апробовані на Українському державному підприємстві поштового зв'язку «Укрпошта» в рамках реалізації в системі поштового зв'язку України проекту «Електронна поштова марка». За матеріалами роботи підготовлена кандидатська дисертація на тему «Методи апаратної реалізації операцій в скінченних полях».

Результати роботи впроваджено в навчальний процес при викладанні дисциплін «Теорія інформації» (підготовлено дві лекції за темами «Методи та засоби виконання операцій у скінченних полях», «Дослідження основних операцій модулярної арифметики» та лабораторну роботу за темою «Дослідження мікрооперацій модулярної арифметики на регістрах») та «Архітектура комп'ютера» (підготовлено лекцію за темою «Архітектура співпроцесора для реалізації обчислень в полях Галуа» та лабораторну роботу за темою «Дослідження засобів апаратної підтримки обчислень за модулем незвідного многочлена»).

За результатами роботи захищено 3 магістерські випускні роботи, 2 дипломні проекти спеціаліста та 5 дипломних робіт бакалавра.

10. Форма участі інвестора (*яка краща форма участі в реалізації результатів проекту інвестора: частка в проекті%, частка від прибутку%, інше*)

Залучення інвестора не передбачається

11. Обсяг інвестицій (*необхідна для результатів проекту сума інвестицій в доларах США*).

12. Мета інвестицій (*розширення бізнесу, створення нового підприємства, інше*).

13. Назва організації, телефон, E-mail

НТУУ «КПІ ім. Ігоря Сікорського», факультет прикладної математики, кафедра програмного забезпечення комп'ютерних систем,

(044) 204-91-13, dychka@scs.ntu-kpi.kiev.ua

14. Фото розробки

Не передбачено побудову макета

15. Перелік публікацій за матеріалами досліджень за період виконання розробки

1. Zhengbing Hu, I. A. Dychka, Onai Mykola, Bartkoviak Andrii, "The Analysis and Investigation of Multiplicative Inverse Searching Methods in the Ring of Integers Modulo M", International Journal of Intelligent Systems and Applications (IJISA), Vol.8, No.11, pp.9-18, 2016. DOI: 10.5815/ijisa.2016.11.02
2. Legeza V.P. Determining the amplitude-frequency response and setting of a nonlinear vibration isolation system with a quasi-isochronous damper // SPRINGER, Intern. Applied Mechanics, 2015, V. 51, №2, – P. 233 – 241.
3. Дичка, І.А. Модифікований віконний метод однократного множення точки еліптичної кривої на скаляр у полі $GF(p)$ / І.А. Дичка, М.В. Онай, Т.П. Дрозда // Науковий журнал "Радіоелектроніка, інформатика, управління". — Запоріжжя. — 2016. — №2. — С. 95-102.
4. Легеза В.П. Подавление колебаний проводов и тросов с использованием двухмассового маятникового гасителя / В.П. Легеза, И.А. Дичка, Я.В. Бовкун // Электрические сети и системы. – 2016. – №2. – С. 7-13.
5. Реалізація неавтономних обчислень в надлишкових системах числення на ПЛІС / В.І. Жабін, В.В. Жабіна, О.В. Скоріченко // Вісник Національного технічного університету України "КПІ". "Інформатика, управління та обчислювальна техніка". – 2016. – №64. – С. 26-33.
6. Analysis of Parallel Computations Efficiency for User's Private Multimedia Data Protection in Clouds / Ivan Dychka, Semen Shyrochyn, Yevgeniya Sulema // Наукові вісті Національного технічного університету України "Київський політехнічний інститут". – 2016. – Випуск 1. – С. 40-46.
7. Бартков'як А.Ю., Соколовська А.В., Заболотня Т.М. Спосіб визначення комплексної оцінки тональності відгуків Інтернет-користувачів // Біоніка інтелекту: наук.-техн. журнал. – 2016. – №1 (86). – С. 8-12.
8. Сулема Є.С. Спосіб стеганографічного захисту даних в аудіо-файлах на основі комплементарного образу / Є. С. Сулема, С. С. Широчин // Вісник КПІ. Інформатика, управління та обчислювальна техніка. – 2014. – Вип. 61. – С. 80-87
9. Mulsemedia Vs. Multimedia: State of the Art and Future Trends" (Invited Paper) / Yevgeniya Sulema // Proceedings of the 23rd IEEE International Conference on Systems, Signals and Image Processing IWSSIP2016. – Bratislava, Slovakia. – 2016. – pp. 19-23.
10. Image Protection Method Based on Binary Operations / Yevgeniya Sulema // Proceedings of the 23rd IEEE International Conference on Systems, Signals and Image Processing IWSSIP2016. – Bratislava, Slovakia. – 2016. – pp. 295-298.
11. Дичка І.А., Шолтун Д.В. Застосування трійкового алгоритму Хаффмана при створенні триколірного графічного коду // ІІ Всеукраїнська науково-практична конференція молодих учених і студентів «Інформаційні технології в освіті, техніці та промисловості», м. Івано-Франківськ, 6 – 9 жовтня 2015 р. : збірник тез доповідей. – Івано-Франківськ, 2015. – С. 103-105
12. Дичка І.А., Шолтун Д.В., Голуб В.І., Ващілін О.В. Автоматична ідентифікація поштових відправлень на основі триколірних цифрових поштових марок // V Міжнародна науково-практична конференція Інфокомунікації – сучасність та майбутнє», м. Одеса, 29 – 30 жовтня 2015 р.: матеріали конференції. – Одеса, 2015. – С. 162-165.
13. Онай, М.В. Спосіб апаратної реалізації операцій над елементами поля $GF(2^m)$ з використанням логарифма Зеча [Текст] / М.В. Онай, А.І. Дичка // Інтелектуальні технології в системному програмуванні (ІТСП-2015). IV Всеукраїнська науково-практична конференція молодих учених та студентів. Збірник наукових праць. Хмельницький, 22-24 квітня 2015 року. — Хмельницький : ПП Гонта А.С., 2015. — С. 51.

14. Онай, М.В. Ефективний алгоритм множення точки еліптичної кривої над основним полем Галуа з використанням системи числення з подвійною основою [Текст] / М.В. Онай, А.В. Соколовська // Інтелектуальні технології в системному програмуванні (ІТСП-2015). IV Всеукраїнська науково-практична конференція молодих учених та студентів. Збірник наукових праць. Хмельницький, 22-24 квітня 2015 року. — Хмельницький : ПП Гонта А.С., 2015. — С. 52.
15. Дичка, І.А. Застосування *k*-арного методу Евкліда для пошуку мультплікативно оберненого елемента у кільці лишків за модулем *m* [Текст] / І.А. Дичка, М.В. Онай, А.Ю. Бартков'як // Матеріали статей П'ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». м. Івано-Франківськ : п. Голіней О.М., 2015. — С. 151-153.
16. Онай, М.В. Скалярне множення точки еліптичної кривої у полі $GF(p)$ з поданням множника у системі числення з подвійною основою [Текст] / М.В. Онай, А.В. Соколовська // Матеріали статей П'ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». м. Івано-Франківськ : п. Голіней О.М., 2015. — С. 178-180.
17. Онай, М.В. Пошук мультиплікативно оберненого елементу у кільці лишків за довільним модулем методами, що грунтуються на модулярному піднесенні до степеня [Текст] / М.В. Онай, А.Ю. Бартков'як // Шістнадцята міжнародна наукова конференція імені академіка Михайла Кравчука, 14-15 травня, 2015 р., Київ : Матеріали конф. Т. 2. Алгебра. Геометрія. Математичний аналіз. — К. : НТУУ "КПІ", 2015. — С. 139-141.
18. Онай, М.В. Знаходження мультиплікативно оберненого елемента у кільці лишків за довільним модулем методом Джої-Пейє [Текст] / М.В. Онай, А.Ю. Бартков'як // Міжнародна науково-практична конференція «Проблеми інформатики та комп'ютерної техніки». Праці конференції. — Чернівці : Видавничий дім "Родовід", 2015. — С. 91-93.
19. Онай, М.В. Віконні методи множення точки еліптичної кривої на число [Текст] / М.В. Онай, А.В. Соколовська // Міжнародна науково-практична конференція «Проблеми інформатики та комп'ютерної техніки». Праці конференції. — Чернівці : Видавничий дім "Родовід", 2015. — С. 93-95.
20. Жабіна, В.В. Реалізація операцій з плаваючею комою в системах з безпосередніми зв'язками між обчислювальними модулями [Текст] / В.В. Жабіна // Міжнародна науково-практична конференція «Проблеми інформатики та комп'ютерної техніки». Праці конференції. — Чернівці : Видавничий дім "Родовід", 2015. — С. 104-106.
21. Онай, М.В. Оцінка стійкості криптографічних протоколів, заснованих на складності задачі дискретного логарифмування у скінченному полі $GF(p^m)$ [Текст] / М.В. Онай, А.І. Дичка // Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації». м. Вінниця, 19-21 квітня 2016 року. – Вінниця : ТОВ "Нілан-ЛТД", 2016. — С. 94-97.
22. Онай, М.В. Дискретне логарифмування у скінченному полі $GF(p)$ та алгебраїчних структурах визначених над ним / М.В. Онай, А.І. Дичка // Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей Міжнародної науково-практичної конференції, 24-25 березня 2016 року, м. Кіровоград : КНТУ, 2016. – С. 56-57.
23. Онай, М.В. Узагальнений метод скалярного множення точки еліптичної кривої над полем $GF(p)$ у системі числення з мультиосновою [Текст] / М.В. Онай, Т.П. Дрозда // Прикладна математика та комп'ютинг. ПМК-2016 : восьма наук. конф. магістрантів та аспірантів, Київ, 20-22 квітня 2016 р. : зб. тез доп. / [ред кол.: Дичка І.А. та ін.] . — К. : Просвіта, 2016. — С. 218-225.

16. Ключові слова до розробки: поле Галуа, скінченне поле, криптографія, завадостійке кодування даних, система команд, процесор Галуа.