Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U004483

Особливі позначки: відкрита

Дата реєстрації: 17-11-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Онай Микола Володимирович
2. Onai Mykola Volodymyrovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 13-11-2017

Спеціальність за освітою: 8.05010301

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.002.02

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Інститут енергозбереження та енергоменеджменту

Код за ЄДРПОУ: 247571500

Місцезнаходження: вул. Борщагівська 115, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.07.05

Тема дисертації:

1. Методи та засоби підвищення ефективності реалізації обчислювальних операцій у скінченних полях

2. Methods and Means of Implementation Efficiency Increasing for Computational Operations in Finite Fields

Реферат:

1. У дисертаційній роботі вирішено актуальну науково-прикладну задачу - підвищення продуктивності систем цифрової обробки даних та криптографічних перетворень, забезпечення завадостійкості зберігання і передачі даних за рахунок створення ефективних технічних засобів для виконання обчислень у скінченних полях шляхом структурно-логічної оптимізації архітектур апаратних засобів, що реалізують процеси виконання операцій у полях Галуа. Запропоновано метод виконання операцій над елементами поля GF(2m). Особливістю даного методу, на відміну від існуючих, є застосування табличного зберігання елементів поля у многочленному та степеневому їх поданні з можливістю розрідженого формування таблиці елементів поля, що зменшує витрати пам'яті для її зберігання. Розроблений метод забезпечує зростання швидкодії на 15% порівняно з існуючим методом. Запропоновано модифікацію методу піднесення до степеня елементів поля GF(p) з ковзним вікном, яка забезпечує приріст швидкодії на 7-9 %. Спроектовано на ПЛІС фірми Xilinx

процесор Галуа, що орієнтований на виконання операцій у скінченних полях виду GF(p) та GF(2m). Запропоновано програмістську модель процесора Галуа, яка дозволяє розробляти програмне забезпечення довільної складності мовою Асемблера процесора Галуа.

2. The thesis is devoted to the problem of increasing the efficiency of computations in finite fields. The proposed solution to this problem is to develop methods and means for performing operations on elements of finite fields GF(p) or GF(2m). The analysis of the current state of the development of methods of operations in finite fields is carried out and priority points are highlighted. It is best to classify them on the basis of the distinguished features. The classification of the methods of performing the most computational expensive operations (the calculation of the multiplicative inverse element and the exponentiation) in the finite fields was per-formed. It enables to conduct thorough research and form the directions of develop-ment for these methods. The method of high-speed implementation of additive and multiplicative opera-tions on elements of GF(2m) and corresponding hardware structures for its implemen-tation are proposed. Additive operations include addition and subtraction. Multiplica-tive operations include multiplication, exponentiation, multiplicative inverse element calculation, and division. The research has shown that table storage of elements of the GF(2m) in their polynomial and power representation ensures the maximum speed and versatility of the arithmetic logic unit. With the use of long integer operands, the sparse formation of the table of field elements is proposed. It enables reducing the memory consumption for its storage in several times. The algorithms for converting power representation into polynomial one and polynomial representation in power one with the use of a sparse table are constructed. The developed method provides a 15% increase in performance comparing with the existing method. The research of the developed Galois processor has been carried out, which showed that this processor provides an increase in the productivity of computing by 27% compared with the universal computing means. A program model of the Galois processor is constructed, which allows the user to create software of arbitrary complexity in Assembler of the Galois processor.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Дичка Іван Андрійович

2. Dychka Ivan Andrijovych

Кваліфікація: д.т.н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Опанасенко Володимир Миколайович
2. Опанасенко Володимир Миколайович

Кваліфікація: д.т.н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Гамаюн Володимир Петрович
2. Гамаюн Володимир Петрович

Кваліфікація: д.т.н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Луцький Георгій Михайлович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Луцький Георгій Михайлович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.