Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0405U003919

Особливі позначки: відкрита

Дата реєстрації: 27-10-2005

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Мекуш Оксана Григорівна
2. Mekush Oksana Grygorivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 01.05.01

Назва наукової спеціальності: Теоретичні основи інформатики та кібернетики

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 20-10-2005

Спеціальність за освітою: 8.080101

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.001.09

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, 60, м. Київ, Київська обл., 01033, 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: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: 01033, м. Київ, вул. Володимирська, 64

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.21

Тема дисертації:

1. Алгоритми модулярної арифметики великих чисел

2. Modular arithmetic algorithms for long numbers

Реферат/анотація:

1. Дисертаційна робота присвячена дослідженню алгоритмів модулярної арифметики. В роботі розроблені нові ефективні алгоритми модулярної арифметики, зокрема з допомогою використання паралельних обчислень. Запропоновано ефективний ітеративний алгоритм модулярної редукції, удосконалено паралельний метод експоненціювання, що базується на представленні експоненти з допомогою лінійних форм числових послідовностей, на основі методів модулярного експоненціювання розроблені два нові паралельні методи модулярного мультиекспоненціювання. Дані алгоритми розв'язують важливу задачу прискорення шифрування - дешифрування інформації в криптографічних системах реального часу та мають істотне значення для розробки математичного та програмного забезпечення сучасних систем захисту інформації.

2. The thesis is devoted to analysis of algorithms aimed at modular arithmetic. New effective modular arithmetic algorithms are proposed, especially with using parallel computations. The effective iterative modular reduction algorithm is proposed, parallel modular exponentiation method based on linear forms of digital sequences was improved, new effective parallel multi-exponentiation methods based on modular exponentiation methods are proposed. These algorithms solve an important task - to speed up encryption-decryption of information in real time cryptography systems and have vital importance for developing software for current information security systems.

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. Анісімов Анатолій Васильович
2. Anisimov Anatoliy Vasilovich

Кваліфікація: д.ф.-м.н., 01.05.01

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. Асельдеров Зайнутдін Макашаріпович

2. Асельдеров Зайнутдін Макашаріпович

Кваліфікація: д.ф.-м.н., 01.05.01

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. Гороховський Семен Самуїлович

2. Гороховський Семен Самуїлович

Кваліфікація: к.ф.-м.н., 01.01.09

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 Закусило Олег Каленикович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Закусило Олег Каленикович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.