Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0499U001575

Особливі позначки: відкрита

Дата реєстрації: 16-10-2000

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Салем Шеріф Ель-фард

2. Salem Sherif El'-fard

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: 24-06-1999

Спеціальність за освітою:

Місце роботи здобувача: 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

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: 27.47.17

Тема дисертації:

1. Порівняльний аналіз методів модулярноє редукціє

2. Comparative Analysis of Modular Reduction Methods

Реферат/анотація:

1. Робота присвячена вивченню складності операціє модулярноє редукціє x mod m для великих чисел. Досліджено п'ять методів:класичний метод, метод Баррета, метод Кнута-Флойда, метод Монтгомері та метод Анісімова А.В. На основі теоретичних досліджень та програмних експериментів зроблено порівняльний аналіз усіх наведених у роботі методів. Розроблено паралельні варіанти обчислення модулярноє експоненти.

2. The thesis is devoted to the study of modular reduction function x mod m for large numbers. This operation is basic for public-key cryptosystems and determines their speed of processing. The research is aimed to comprehensively analyze modular reduction methods from the viewpoint of computation complexity. The general aim of the research is as follows: to create new effective algorithms for solving modular reduction problems for large numbers; to do comparative analysis of known modular reduction methods with the purpose to choose the

fastest and most suitable for use in public-key cryptography; to prove theoretically correctness of some concrete modular reduction methods; to create new parallel algorithms for modular exponention of large numbers; to fulfill computer experiments for comparison of modular reduction methods.

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 А.В.

2. Анісімов А.В.

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 З.М.

2. Асельдеров З.М.

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. Проценко В.С.

2. Проценко В.С.

Кваліфікація: к.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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Бублик Б.М.

Власне Прізвище Ім'я По-батькові головуючого на засіданні Бублик Б.М.

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.