Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U001579

Особливі позначки: відкрита

Дата реєстрації: 18-10-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Місько Віталій Миколайович
2. Misko Vitalii Mykolaiovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 01.05.02

Назва наукової спеціальності: Математичне моделювання та обчислювальні методи

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 30-09-2019

Спеціальність за освітою: 7.05010101

Місце роботи здобувача: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Код за ЄДРПОУ: 05516949

Місцезнаходження: 03164, Україна, Київ, вул. Генерала Наумова, 15

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.185.01

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Код за ЄДРПОУ: 05516949

Місцезнаходження: 03164, Україна, Київ, вул. Генерала Наумова, 15

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.17.19

Тема дисертації:

1. Обчислювальні методи на основі квадратичного решета при криптоаналізі RSA алгоритму апаратно-програмними засобами.

2. Computational methods based on a quadratic sieve for cryptanalysis of RSA algorithm using hardware and software solution.

Реферат:

1. Метою роботи є зменшення обчислювальної складності методів факторизації багаторозрядних чисел, заснованих на ідеях методу квадратичного решета. Вперше розроблено метод множинного квадратичного k-решета (MQkS), метод діагоналізації матриці "на ходу", метод визначення достатньої кількості B - гладких чисел, метод умовно B-гладких чисел. Запропоновано способи реалізації методу MQkS на апаратно-програмних засобах. Результати роботи дозволяють додати ще один етап криптоаналізу RSA апаратно-програмними засобами, як наслідок, збільшити ефективність криптоаналізу комерційних та державних експертиз у сфері КЗІ нових криптоалгортимів.

2. The purpose of this work is to reduce the computational complexity of the methods of factorization of multi-digit numbers based on the ideas of the quadratic sieve method. For the first time, the method of multiple

quadratic k-sieve (MQkS), the method of diagonalization of the matrix "on the fly", the method of determining a sufficient number of B - smooth numbers, the method of conditionally B-smooth numbers are developed. Methods for implementing the MQkS method on hardware and software are proposed. The results of the work allow us to add another stage of RSA cryptanalysis by hardware and software, as a consequence, to increase the efficiency of cryptanalysis of commercial and state expertise in the field of new cryptocurrencies.

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. Винничук Степан Дмитрович
2. Vynnychuk Stepan Dmytrovych

Кваліфікація: д.т.н., 01.05.02, 01.05.02

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. Каліновський Яків Олександрович

2. Каліновський Яків Олександрович

Кваліфікація: д.т.н., 01.05.02

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. Зінченко Ярослав Вікторович
2. Зінченко Ярослав Вікторович

Кваліфікація: д.т.н., 01.05.02, 01.05.02

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 Мохор Володимир Володимирович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Мохор Володимир Володимирович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.