Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U002884

Особливі позначки: відкрита

Дата реєстрації: 29-09-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Максименко Євген Васильович
2. Maksymenko Yevhen Vasylovych

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: 14-09-2017

Спеціальність за освітою: 7.092401

Місце роботи здобувача: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 34979237

Місцезнаходження: 03056, м. Київ, вул Верхньоключова, 4

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 26.185.01

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: 27.41

Тема дисертації:

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

2. The Computational methods based on the algorithm of Fermat's factorization method during cryptanalysis of RSA algorithm by hardware and software methods

Реферат/анотація:

1. Об'єкт дослідження: процес факторизації багаторозрядних чисел при криптоаналізі RSA-алгоритму. Предмет дослідження: обчислювальні методи факторизації багаторозрядних чисел, що засновані на алгоритмі Ферма та використовують методи проріджування і зменшення обчислювальної складності операцій з багаторозрядними числами. Мета: зниження обчислювальної складності методів факторизації багаторозрядних чисел для підвищення швидкодії апаратно-програмних засобів при вирішенні завдань криптоаналізу RSA алгоритму. Методи дослідженя: методи теорії чисел, теорії оптимізації, алгоритмічної теорії багаторозрядних чисел, теорії складності обчислень, чисельні методи, методи комп'ютерного моделювання. Дисертаційна робота присвячена удосконаленню обчислювальних методів факторизації на основі алгоритму Ферма, які використовуються при проведенні досліджень криптоалгоритмів та протоколів

на основі створення більш ефективних методів проріджування і зменшення обчислювальної складності операцій з багаторозрядними числами. Результати роботи дозволяють підвищити швидкодію апаратно-програмних засобів, які використовуються для проведення тематичних досліджень засобів криптографічного захисту інформації і протоколів на основі RSA-алгоритму.

2. Object of research: The process of factorization of multi-digit numbers during cryptanalysis of the RSA algorithm. Research subject: Computational methods of factorization of multi-digit numbers, based on the Fermat algorithm and using effective methods of thinning and reducing the computational complexity of operations with multi-digit numbers. The aim of research: Reducing the computational complexity of factorization methods for multi-digit numbers to improve the performance of hardware and software in solving RSA algorithm cryptanalysis tasks. Research methods: methods of number theory, optimization theory, algorithmic theory of multi-digit numbers, theory of complexity computation, numerical methods, methods of computer modeling. Dissertation is devoted to the improvement of computing factorization methods based on the Fermat's algorithm, which are used in the research of cryptographic algorithms and protocols which are used in the means and complexes of cryptographic protection of information (CPI) based on the creation of more effective methods of screening and reducing the computational operations of complex multi-digit numbers. The results of the work allow to increase the speed of hardware and software which are used for conducting thematic researches of means for cryptographic information protection and protocols based on RSA-algorithm.

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. Vinnichuk 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, 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. Грищук Руслан Валентинович

2. Грищук Руслан Валентинович

Кваліфікація: д.т.н., 05.13.21, 21.05.01

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	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.