Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U003074

Особливі позначки: відкрита

Дата реєстрації: 07-05-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Мартиненко Сергій Олегович
2. Martynenko Sergii Olegovych

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: 21-03-2012

Спеціальність за освітою: 7.090802

Місце роботи здобувача: Товариство з обмеженою відповідальністю "Телерадіозв'язок"

Код за ЄДРПОУ: 22618433

Місцезнаходження: 61166, Україна, м. Харків, вул. Новгородська, 44, к. 147

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 64.052.01

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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: Харківський національний технічний університет сільского господарства

Код за ЄДРПОУ: 00493741

Місцезнаходження: 61002, Україна, м. Харків, вул. Артема, 44

Форма власності:

Сфера управління: Міністерство освіти і науки, молоді та спорту України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.07.05

Тема дисертації:

1. Метод і засоби зниження обчислювальної складності криптографічних RSA-перетворень на основі модулярної системи числення

2. Method and tools for reducing the computational complexity, cryptography RSA-transformations on the basis of modular number system

Реферат:

1. Об'єкт дослідження - процес обробки криптографічної інформації в модулярній системі числення (МСЧ). Мета дослідження - розробка моделей та методів зниження обчислювальної складності RSA криптоперетворень за рахунок використання адитивно-мультиплікативних властивостей полів Галуа. Методи дослідження - аналіз і синтез, теорія чисел - під час розробки методів і засобів реалізації арифметичних операцій в полях Галуа на основі застосування модулярної системи числення шляхом використання принципу кільцевого зрушення, а також під час розробки методу вибору основ МСЧ; теорія ймовірностей і теорія надійності - під час дослідження методів підвищення безвідмовності спецпроцесора обробки криптографічної інформації (СОКІ), що функціонує в модулярній системі числення. Апаратура - персональний комп'ютер. Теоретичні і практичні результати досліджень - розроблений у дисертаційній

роботі метод зниження обчислювальної складності RSA-криптоперетворень, а також вдосконалені методі виконання арифметичних операцій у модулярній системі числення, шляхом урахування властивостей полів Галуа, є науково-методологічною основою для практичного створення СОКІ в МСЧ. Наукова новизна - вперше запропоновано метод обробки криптоперетворень RSA, який характеризується використанням принципу кінцевого зрушення та базується на застосуванні модулярної системи числення, що дозволяє зменшити обчислювальну складність RSA криптографічних перетворень; удосконалено математичну модель безвідмовності спецпроцесора обробки криптографічної інформації, яка відрізняється урахуванням надійності контрольних трактів, що дає можливість оцінити надійність спецпроцесора обробки криптографічної інформації; удосконалено метод виконання цілочисельних арифметичних операцій в модулярній системі числення, який на відміну від аналогів ураховує адитивно-мультиплікативні властивості полів Галуа, що дозволяє підвищити швидкодію СОКІ. Результати дисертаційної роботи впроваджені у ЗАТ "Інститут інформаційних технологій" (м. Харків) та у Державному підприємстві Харківський приладобудівний завод імені Т.Г. Шевченка (м. Харків). Наукові теоретичні та практичні результати дисертаційної роботи можуть використовуватися у науково-технічних розробках та при проектуванні спецпроцесора обробки криптографічної інформації, що реалізує операції додавання, віднімання, множення та піднесення чисел до квадрата за модулем.

2. Object of research - process of cryptographic information processing in the modular number system. Research objective - The models and method development to reduce RSA cryptotransformation computation complexity through the use of additive-multiplicative propertied of Galois fields. Research methods are based on analysis and synthesis, theory of numbers during development methods and tools of arithmetic operations in the Galois fields by applying modular number system using the principle of circular shift and method of bases choice in the modular number system, probability theory and reliability theory during the study methods of increasing reliability of the special processor handling cryptographic information (SPHCI) which operates in the modular number system. Equipment - the personal computer. Theoretical and practical results of research - the developed in the dissertation method of reducing RSA cryptotransformation computation complexity and improved methods of performing arithmetic operations in the modular number system by considering the properties of Galois fields is a scientific and methodological basis for practical creation of SPHCI in the modular number system.. Scientific novelty - for the first time developed a method for processing of cryptotrasformations, which is based on the use of a modular system by using the principle of circular shift, which reduces the computational complexity of the RSA cryptographic; improved mathematical model of the fail-safe for the special processor handling cryptographic information which is different considering the reliability of the control tracts, which makes it possible to assess the reliability of special processor handling of cryptographic information; improved method for performing integer arithmetic in the modular number system, which is unlike analogues takes into account the additive-multiplicative properties of Galois fields, thus increasing the speed of processing special processor cryptographic information Results of dissertational work are introduced in the closed joint-stock company. "Institute of information technologies" (Kharkov) and Public Enterprise Kharkov Instrumental Factory T.Shevchenko (Kharkov). Scientific theoretical and practical results of the dissertation can be used in the research, design and development special processor handling cryptographic information that implements operations of addition, subtraction, multiplication, and squaring numbers by modulo.

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. Краснобаєв Віктор Анатолійович

2. Krasnobajev Viktor Anatolijovych

Кваліфікація: д.т.н., 20.02.14

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. Кривуля Геннадій Федорович

2. Кривуля Геннадій Федорович

Кваліфікація: д.т.н., 05.13.06

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. Кузнецов Олександр Олександрович

2. Кузнецов Олександр Олександрович

Кваліфікація: д.т.н., 05.13.21

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 Бондаренко Михайло Федорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Бондаренко Михайло Федорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.