Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U003724

Особливі позначки: відкрита

Дата реєстрації: 20-06-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Махмалі Саїдреза

2. Makhmali Saiedreza

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: 11-06-2012

Спеціальність за освітою: 8.091501

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

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 26.002.02

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Інститут енергозбереження та енергоменеджменту

Код за ЄДРПОУ: 247571500

Місцезнаходження: вул. Борщагівська 115, м. Київ, Київська обл., 03056, 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: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи підвищення ефективності захисту інформації та корекції помилок при її передачі з застосуванням алгебри поліноміального множення

2. Methods for increase the efficiency of data protection and transmission error correction by using of polynomial multiplication algebra

Реферат:

1. Дисертація присвячена проблемі підвищення ефективності захисту інформації в комп'ютерних системах і корекції помилок обміну даними між їх компонентами за рахунок прискорення обчислень, пов'язаних з реалізацією захисту даних та корекції помилок їх передачі. На основі досліджень властивості поліноміального квадрату запропоновано метод прискореного експоненціювання на полях Галуа. На основі запропонованого підходу розроблені модифікації методів FFSIS, Шнора та Гіллоу-Квіскватера. Доведено, що запропонований підхід дозволяє прискорити процеси ідентифікації. Запропоновано модифікацію способу формування цифрового підпису DSS на основі використання арифметики кінцевих полів. Розроблено технології генерації ключів, формування цифрового підпису та його перевірки. Запропоновано новий метод

для корекції пачки помилок в каналах зі спектральною модуляцією, особливістю якого є використання математичних операцій без міжрозрядних переносів. Доведено, що запропонований метод забезпечує суттєве прискорення кодування, виявлення та корекції "пачки" помилок, а також спрощення схеми апаратної реалізації.

2. Thesis is dedicated to a problem of increasing of efficiency of data protection in computer system and correcting of errors which appearances during data transmission between of system components by accelerating of calculation necessitates for data protection and transmission errors correction implementation. The lack of necessity of carry processing make possible to simplify and speed up software and hardware implementation. Based on a study of polynomial squaring properties the new method of shortcut exponentiation on Galois fields is proposed. The approach to speed up of zero-knowledge identification of abonents by using of multiplication without carry on Galois fields is proposed. Base on ones modifications of FFSIS, Schnorr and Guillou-Quisquater identification schemes are worked out. It was proved that approach allows to speed up of identification. The techniques of keys generation, forming and verification of signature based of finite fields arithmetic are worked out. The method for burst error correction in spectral modulation channels is proposed, feature of one is use of mathematical operations without carry. It has been shown that proposed method provides a significant acceleration bust errors coding, detection and correction and simplifies hardware implementation.

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. Марковський Олександр Петрович

2. Markovskyy Olexander Petrovich

Кваліфікація: к.т.н., 05.13.05

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. Алішов Надір Ісмаїл-Огли

2. Алішов Надір Ісмаїл-Огли

Кваліфікація: д.т.н., 05.13.05

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. Мартинова Оксана Петрівна

2. Мартинова Оксана Петрівна

Кваліфікація: к.т.н., 05.13.05

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	Луцький Георгій Михайлович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Луцький Георгій Михайлович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.