Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U003528

Особливі позначки: відкрита

Дата реєстрації: 11-06-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Фесенко Андрій В'ячеславович
2. Fesenko Andrij Vyacheslavovech

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: 14-05-2015

Спеціальність за освітою: 8.05010101

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 26.001.09

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: 28.25.23

Тема дисертації:

1. Аналіз складності задачі обернення локально комутативного відображення в класичній і квантовій моделях обчислень.

2. Complexity analysis of the locally commutative mapping inverting problem in classical and quantum models of computation.

Реферат:

1. Дисертаційна робота присвячена побудові загальної алгебраїчної моделі, що поєднує задачі, які виникають при криптоаналізі криптографічних систем і протоколів за допомогою алгебраїчних моделей, та алгебраїчні задачі, які досліджуються в квантовій моделі обчислень. Введено поняття сильно та слабо локально комутативного відображень і показано, що існування важкооборотної функції з такими властивостями є необхідною умовою для побудови багатьох криптографічних систем та протоколів, стійких при теоретико-складносному підході. Введено клас багатоосновних алгебраїчних систем як узагальнення алгебраїчної моделі комутативного симетричного шифру та проаналізовано їх властивості, що дозволило довести існування зведення задачі обернення локально комутативного відображення до алгебраїчних задач таких як

задача про приховану дію на торсорі над абелевою групою. Доведено зведення представлених задач до задачі про прихований зсув, завдяки чому побудовано критерії існування ефективного розв'язку задачі обернення локально комутативного відображення в квантовій моделі обчислень.

2. The thesis is devoted to the construction of general algebraic model to combine problems which are considered by cryptanalysis of cryptographic systems and protocols with algebraic models, and algebraic problems which are investigated in quantum model of computation. The concept of strongly and weakly locally commutative mappings was introduced and shown that the existence of a one-way function with such properties is a necessary condition to construct many cryptographic protocols which would be secure in complexity-theoretic model. A class of heterogeneous algebraic systems was proposed as a generalization of the commutative symmetric cipher's algebraic model and their properties were analyzed, proving the existence of a reduction the locally commutative mapping inverting problem to algebraic problems such as the hidden action on torsor over abelian group problem. Proved a reduction of proposed problems to the hidden shift problem which allows to construct criteria of effective solution's existence for the locally commutative mapping inverting problem in quantum model of computation.

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. Савчук Михайло Миколайович
2. Savchuk Myhajlo Mykolajovych

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. Кнопов Павло Соломонович
2. Кнопов Павло Соломонович

Кваліфікація: д.ф.-м.н., 01.01.09

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. Кулага Анатолій Анатолійович
2. Кулага Анатолій Анатолійович

Кваліфікація: к.ф.-м.н., 01.05.03

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 Анісімов Анатолій Васильович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Анісімов Анатолій Васильович

Відповідальний за підготовку облікових документів

Реєстратор

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