Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U005694

Особливі позначки: відкрита

Дата реєстрації: 18-10-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сіренко Ольга Олександрівна
2. Sirenko Olga Oleksandrivna

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: 26-09-2013

Спеціальність за освітою: 8.04020101

Місце роботи здобувача: Публічне акціонерне товариство "УкрСиббанк"

Код за ЄДРПОУ: 09807750

Місцезнаходження: 79000, м. Львів, вул. Куліша, 28

Форма власності:

Сфера управління: Національний банк 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: 49.03.07

Тема дисертації:

1. Алгебраїчні методи аналізу стійкості блокових симетричних криптоалгоритмів

2. Algebraic methods for stability analysis of block symmetric encryption algorithms

Реферат/анотація:

1. Дисертаційна робота містить нові теоретичні дослідження в галузі побудови надійних систем захисту інформації та новий підхід щодо аналізу стійкості блокових симетричних криптоалгоритмів до сучасних методів криптоаналізу, що базуються на методі гомоморфізмів, та атак зрізаних диференціалів. Оскільки на сьогоднішній день важливе місце серед засобів захисту інформації займають симетричні блокові криптоалгоритми, головною перевагою яких є їх швидка програмна реалізація, то важливим та актуальним питанням є дослідження їх стійкості до різних сучасних атак, зокрема до групового та різницевого криптоаналізу. Як правило, їх стійкість до методів гомоморфізмів визначається алгебраїчними властивостями різних груп підстановок, що пов'язані з системою раундових шифруючи перетворень даного шифру. Дана робота присвячена дослідженню алгебраїчних властивостей групи підстановок, що породжується раундовими функціями, а саме "перемішувальним" властивостям групових операцій, що задані

на множині відкритих текстів.

2. The Thesis contains new theoretical research in building reliable informational systems and a new approach to analysis of stability of the block symmetric encryption algorithms and modern methods of cryptanalysis, based on the method of homomorphism and truncated differential cryptanalysis . Symmetrical block cryptoalgorithms take an important place in modern information security. One of their main advantages is relatively fast software implementation, and that's why studying their resistance to various modern attacks, particularly the group and differential cryptanalysis, is an important and urgent issue. Normally, their resistance to the homomorphism methods is defined by the algebraic properties of different groups of substitutions that in turn are related to the system of round encrypting transformations of a given cipher. This work is dedicated to the study of algebraic properties of permutations that are generated by round functions, particularly "mixing" properties of the group operations, which are defined on a set of plain text data.

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. Задірака Валерій Костянтинович
2. Zadiraka Valeriy Kostantinovich

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. Савчук Михайло Миколайович

2. Савчук Михайло Миколайович

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

Власне Прізвище Ім'я По-батькові:

1. Кругляк Станіслав Аркадійович

2. Кругляк Станіслав Аркадійович

Кваліфікація: д.ф.-м.н., 01.01.06

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.