Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0414U003047

Особливі позначки: відкрита

Дата реєстрації: 13-05-2014

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Казимиров Олександр Володимирович
2. Kazymyrov Oleksandr Volodymyrovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 22-04-2014

Спеціальність за освітою: 8.160101

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

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): К 64.052.05

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 університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

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 та засоби генерації нелінійних вузлів заміни для симетричних криптоалгоритмів

2. Methods and techniques of generation of nonlinear substitutions for symmetric encryption algorithms

Реферат/анотація:

1. Дисертація присвячена розробці методів побудови вузлів нелінійної заміни для симетричних криптопримітивів з оптимальними криптографічними показниками стійкості. У роботі пропонуються декілька методів формування підстановок як для відомих, так і для перспективних симетричних криптоалгоритмів. Запропоновані методи засновані на критеріальному підході з використанням теорії векторних булевих функцій. Виходячи з алгебраїчного криптоанализа шифрів, представлених на український конкурс, був розширений критерій алгебраїчного імунітету, а також доданий критерій приналежності кількох підстановок до різних класів еквівалентності. Показується, що застосування підстановок, згенерованих на основі запропонованих методів у відзначеному алгоритмі блокового симетричного шифру "Калина", що був представлен на національний конкурс з вибору перспективного алгоритму шифрування, дозволяє збільшити нелінійність з 96 до 104 при збереженні на високому рівні всіх інших показників. Запропоновано конкретні підстановочні конструкції для застосування в симетричних криптоалгоритмах. Результати практичного застосування запропонованих методів з використанням кластера підтверджують ефективність генерації

підстановок нового типу

2. New methods of constructing nonlinear substitutions, which are used in symmetric cryptographic primitives, with optimal properties are presented in the thesis. Several methods of substitutions' generation for both existing and prospective symmetric cryptographic algorithms are proposed. These methods are based on the criteria approach using the theory of vectorial Boolean functions. Based on the algebraic cryptanalysis of ciphers submitted to the Ukrainian competition, the extended algebraic immunity criterion and the criterion for multiple substitutions belonging to different equivalence classes were taken into account in the search procedure. Proposed methods allow to increase the non-linearity from 96 to 104. The usage of such substitutions in the block cipher "Kalyna", which was noted in the national competition for selection of prospective encryption algorithm, gives a high level resistance to all known attacks. Efficiency of the new methods confirmed by practical search using a cluster system, which allows to find specific substitution constructions for symmetric cryptoalgorithms.

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. Олійников Роман Васильович
2. Oliynykov Roman Vasylyovych

Кваліфікація: к.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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Толюпа Сергій Васильович

2. Толюпа Сергій Васильович

Кваліфікація: д.т.н., 05.12.02

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. Конюшок Сергій Миколайович

2. Конюшок Сергій Миколайович

Кваліфікація: к.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 Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.